ELSEVIER

Theoretical Computer Science 215 (1999) 1–30

Theoretical Computer Science

Fundamental Study

Length of prime implicants and number of solutions of random CNF formulae

Y. Boufkhad *, O. Dubois

LIP6, Box 169, CNRS-Université Paris 6, 4 place Jussieu, 75252 Paris cedex 05, France

Communicated by M. Nivat

Abstract

Consider a uniform distribution of r-CNF formulae (in Conjunctive Normal Form) with cn clauses, each with r distinct literals, over a set of n variables. A prime implicant $\mathscr{I}$ of a formula Φ is a consistent conjunction of literals which implies Φ but ceases to imply when deprived of any one literal. The normalized length of $\mathscr{I}$ is the ratio of the number of its literals to the number of variables occurring in Φ. We show that for any $\varepsilon>0$ and for some range of values of c depending on r, almost every r-CNF formula:

- either is satisfiable and any one of its prime implicants has a normalized length at least equal to $(\alpha_m^r(c)/(1-e^{-rc}))-\varepsilon$ and at most equal to $(\alpha_M^r(c)/(1-e^{-rc}))+\varepsilon$, $\alpha_m^r(c)$ and $\alpha_M^r(c)$ being well-defined as functions of c,
  or is unsatisfiable.

A first practical consequence is when testing the satisfiability of r-CNF formulae by procedures such as the well-known Davis, Putnam and Loveland Procedure, for almost every r-CNF formula, when it is satisfiable, the proportion of variables which must be assigned a value by such procedures, in order to find a solution, is at least equal to $(\alpha_m^r(c)/(1-e^{-rc}))-\varepsilon$.

A second consequence is that almost every r-CNF formula, when it is satisfiable, has an exponential actual number of solutions (i.e. the number of solutions defined on the variables occurring in the formula) at least equal to $2^{(1-e^{-rc}-\alpha_M^r(c)-\varepsilon)n}$. Moreover for $r=2,3$ we show that for any c it is at least equal to $2^{0.03n}, 2^{0.012n}$, respectively.

Keywords: Satisfiability; Prime Implicants; Number of Solutions; Davis and Putnam

Contents

* Corresponding author. E-mail: yacine.boufkhad@lip6.fr.

0304-3975/99/$ – see front matter
PII: S0304-3975(95)00184-4

1. Introduction

A CNF formula is a conjunction of clauses, each clause being a disjunction of literals over a set of variables. A literal is a boolean variable x or its negation $\neg x$. A truth assignment is a mapping which assigns 1 or 0 to each variable in its domain. A CNF formula Φ over a set of n variables is satisfiable or consistent iff there exists a truth assignment w under which Φ has the value 1. w is called a solution of Φ. Determining whether a given CNF formula is satisfiable is the well-known Satisfiability Problem (SAT for short).

An r-CNF formula has clauses, each with exactly r literals. As is well-known, to test the satisfiability of 2-CNF formulae is a problem in P, and for $r \geqslant 3$ the problem is NP-complete. r-CNF formulae are currently under active study because for $r \geqslant 3$, they provide an inexhaustible source of difficult tests for the design of efficient algorithms solving the SAT Problem [5, 2]. The general probabilistic model used to generate these formulae consists in choosing uniformly, independently and with replacement a given number m of clauses from the $2^r\binom{n}{r}$ possible clauses with r distinct variables over a set of n boolean variables. Throughout this paper the ratio number of clauses to number of variables of formulae is denoted by c and this probabilistic model is denoted by $\Omega(n,c,r)$. For these formulae, experiments provide evidence for a threshold phenomenon in the following sense. Almost every (a.e.) formula in $\Omega(n,c,r)$ would be satisfiable for c smaller than a well-defined constant c_r^* depending on r and unsatisfiable for c greater than c_r^* [7, 12, 5, 2]. The phrase "Almost every (a.e.) formula in $\Omega(n,c,r)$ has a given property $\mathscr{P}$" means as usual, that the probability to have $\mathscr{P}$ tends to 1 as n tends to infinity. Up to now, only the threshold for 2-CNF formulae has been demonstrated to be at $c=1$ by Chvàtal and Reed [1] and Goerdt [8]. From experiments the value of c_3^* is expected to be at about 4.25.

A prime implicant (PI for short) of a CNF formula Φ is a consistent conjunction $\mathscr{I}$ of literals which logically implies Φ ($\mathscr{I} \Rightarrow \Phi$) but ceases to when $\mathscr{I}$ is deprived of any one literal [18–20]. We call length of a PI, the number of its literals. PIs of boolean formulae have been used in many areas, such as digital circuit optimization [19, 15], fault trees [9], assumption truth maintenance systems [4, 21], knowledge compilation [22, 14]. This paper is concerned with the lengths of prime implicants of satisfiable r-CNF formulae in $\Omega(n,c,r)$. Not all n variables may occur in a random formula of $\Omega(n,c,r)$. And the length of a PI is meaningful only if it is compared with the number

of variables occurring in the formulae. It is not therefore sufficient to consider simply the length of a PI of a formula of $\Omega(n,c,r)$. So we define a *normalized length* of a PI. First we call *actual number of variables* of any CNF formula F, the number of distinct variables occurring in F. It follows that we call the *actual number of solutions* of F, the number of its solutions defined over the set of variables occurring in F.

Definition 1.1. The normalized length of a prime implicant of F is the ratio of the number of its literals to the actual number of variables of F.

In this paper we establish non-obvious upper and lower bounds on the normalized length of PIs of a.e. satisfiable formula in $\Omega(n,c,r)$. The phrase "a.e. satisfiable formula in $\Omega(n,c,r)$ has a given property $\mathscr{P}$" will mean, throughout the paper, that the ratio of the number of satisfiable formulae not satisfying $\mathscr{P}$ (or equivalently the number of formulae which either are satisfiable and have $\mathscr{P}$, or are unsatisfiable) to the total number of formulae, satisfiable and unsatisfiable, in $\Omega(n,c,r)$ tends to 0 (respectively 1) as n increases indefinitely. Of course the established bounds concern the formulae with a ratio c, number of clauses to number of variables, at most equal to the value of the supposed (demonstrated for $r=2$) threshold since, beyond the threshold a.e. formula is unsatisfiable. 0 and 1 are obvious lower and upper bounds of the normalized length. The bounds presented in this paper are established by calculating from Definition 1.1, on the one hand, lower and upper bounds of the actual number of variables of a.e. formula in $\Omega(n,c,r)$, and on the other hand, lower and upper bounds of the number of literals of PIs of a.e. satisfiable formula in $\Omega(n,c,r)$.

Tight bounds on the actual number of variables can be easily obtained by using a classical result on the proportion of empty urns after a random allocation of balls in urns [10, 11, 17]. For this, consider the following modified probabilistic model. A random r-CNF formula with cn clauses is obtained by choosing uniformly, independently, and with replacement, r variables from a set of n variables and then by negating, with probability 1/2, each of the r chosen variables to form every clause of the formula. This modified probabilistic model differs from the model $\Omega(n,c,r)$ by the replacement of each of the r variables chosen to form every clause of a formula. Denoting by Λ the actual number of variables of a random formula of the modified probabilistic model, from the result cited above on the proportion of empty urns in the urn model, we can then deduce that for n large, Λ is concentrated around the mean $(1-\mathrm{e}^{-rc})n$, i.e., for any $\varepsilon>0$:

$$\lim_{n\to\infty} \mathbf{Pr}\left(\left|\frac{\Lambda}{n}-(1-\mathrm{e}^{-rc})\right|>\varepsilon\right)=0.$$

From this, it is an easy exercise to get the same result for the model $\Omega(n,c,r)$. Hence:

Proposition 1.1. *For any $\varepsilon>0$, almost every formula in $\Omega(n,c,r)$ has an actual number of variables bounded by $(1-\mathrm{e}^{-rc}-\varepsilon)n$ and $(1-\mathrm{e}^{-rc}+\varepsilon)n$.*

0 and n are the obvious lower and upper bounds of the length of PIs of satisfiable formulae of $\Omega(n,c,r)$. For $c<1$, a better upper bound than n is cn since, as we will see in Section 2, the number of literals of a PI of a CNF formula cannot be larger than the number of clauses. We can provide better lower and upper bounds by applying the first moment method to the number of PIs, with a given length, of a random formula in $\Omega(n,c,r)$. Let αn be a length of PI with $0\leqslant\alpha\leqslant\inf(1,c)$ and let $\mathscr{PI}^{\alpha n}_{r,c,n}$ be the set of PIs, with length αn, of a random formula of $\Omega(n,c,r)$. We will calculate in Section 2, the exponential order of the expectation of $|\mathscr{PI}^{\alpha n}_{r,c,n}|$ with $\alpha>0$:

Proposition 1.2.

$$\mathbf{E}(|\mathscr{PI}^{\alpha n}_{r,c,n}|)\asymp[f_{r,c}(\alpha)]^n$$

with

$$f_{r,c}(\alpha)=(1-\alpha)^{-(1-\alpha)}\left(\frac{2(e^{x_0}-1)}{\alpha}\right)^{\alpha}e^{(\zeta_r(\alpha)/\kappa_r(\alpha))x_0-c}\left(\frac{c\kappa_r(\alpha)}{x_0\phi_r}\right)^{c} \tag{1.1}$$

x_0 being the unique positive root of the equation below if $\alpha\neq c$ and the obvious unique root 0 if $\alpha=c$:

$$1-e^{-x}-\frac{\alpha x}{c-x\,\zeta_r(\alpha)/\kappa_r(\alpha)}=0. \tag{1.2}$$

$\kappa_r(\alpha),\zeta_r(\alpha),\phi_r$ being defined respectively as follows:

$$\kappa_r(\alpha)=\frac{(2-\alpha)^{r-1}}{(r-1)!},\quad \zeta_r(\alpha)=\frac{2^r-(2-\alpha)^r-\alpha r(2-\alpha)^{r-1}}{r!},\quad \phi_r=\frac{2^r}{r!}. \tag{1.3}$$

We show that on $[0,\inf(1,c)]$, $f_{r,c}(\alpha)$ first increases, attains an absolute maximum at some value denoted by $\widehat{\alpha}_{r,c}\in]0,\inf(1,c)[$ and then decreases. Assume first that for a fixed r and a given c, the maximum $f_{r,c}(\widehat{\alpha}_{r,c})$ is less than 1. Then from the fact that the expectation of PIs of any length is such that: $\mathbf{E}(|\mathscr{PI}_{r,c,n}|)\asymp[f_{r,c}(\widehat{\alpha}_{r,c})]^n$, it easily follows that a.e. formula in $\Omega(n,c,r)$ is unsatisfiable. Now assume that for a fixed r and for some c, the maximum of $f_{r,c}(\widehat{\alpha}_{r,c})$ is higher than 1, and assume further that, according to the variations of $f_{r,c}(\alpha)$, $f_{r,c}(\alpha)$ intersects $y=1$ at two points denoted by $\alpha^r_m(c)$ and $\alpha^r_M(c)$ such that $0<\alpha^r_m(c)\leqslant\widehat{\alpha}_{r,c}\leqslant\alpha^r_M(c)<\inf(1,c)$ and $f_{r,c}(\alpha^r_m(c))=f_{r,c}(\alpha^r_M(c))=1$. Using the exponential order of the expectation, it can be easily shown that for any $\varepsilon>0$, almost no formula in $\Omega(n,c,r)$ has a PI with a length lower than $(\alpha^r_m(c)-\varepsilon)n$ or greater than $(\alpha^r_M(c)+\varepsilon)n$. Those numbers represent therefore respective lower and upper bounds of the length of PIs of a.e. satisfiable formulae in $\Omega(n,c,r)$. It is therefore crucial to know whether $f_{r,c}(\alpha)$ intersects the line $y=1$ at two, one or zero points.

By merely using the intermediate value theorem, we will show in Section 3 that for any $r\geqslant 2$ and every $c>0$ there exists a point $\alpha^r_m(c)$ satisfying the conditions mentioned above. We can then deduce a lower bound of the normalized length of PIs which is $\alpha^r_m(c)/(1-e^{-rc})-\varepsilon$. This result is stated in our theorem on the lower bound:

Theorem 1.3 (Lower bound). *For any $\varepsilon>0$ and for every $c>0$, almost every formula in $\Omega(n,c,r)$:*

- *either is satisfiable and any one of its prime implicants has a normalized length greater than $(\alpha_m^r(c)/(1-\mathrm{e}^{-rc}))-\varepsilon$, where $\alpha_m^r(c)$ is the lower root of $f_{r,c}(\alpha)=1$,*
- *or is unsatisfiable.*

This theorem has a practical consequence for the procedures which test satisfiability of r-CNF formulae by assigning values to the variables, as does the classical Davis, Putnam and Loveland (DPL) procedure [3, 13]. The shortest PI of a satisfiable formula represents the smallest number of variables to be assigned a value to satisfy every clause of the formula. Consequently, for any small $\varepsilon>0$, a procedure testing satisfiability such as DPL, must, to find a solution of a.e. satisfiable formula in $\Omega(n,c,r)$, assign a correct value to a proportion of variables occurring in the formula at least equal to $(\alpha_m^r(c)/(1-\mathrm{e}^{-rc}))-\varepsilon$. It can be observed numerically that $\alpha_m^r(c)$ increases as a function of c (see Tables 1–3,5, Section 3). Consequently, the minimum number of variables which must be assigned a correct value in order to find a solution, increases as a function of c. This supports the experimental fact that for a given number of variables the difficulty of finding a solution of a satisfiable random formula in $\Omega(n,c,r)$ with a procedure such as DPL, increases as a function of the number of clauses [16, 2, 5].

We now sketch the calculation of the upper bound. The situation is more complicated than for the lower bound. To obtain a non-obvious upper bound of the normalized length of PIs, it is not sufficient that $f_{r,c}(\alpha)$ intersects the line $y=1$ at a point $\alpha_M^r(c)$ such that $\widehat{\alpha}_{r,c}\leqslant\alpha_M^r(c)<\inf(1,c)$. For $\varepsilon>0$ as small as we want, $(\alpha_M^r(c)+\varepsilon)n$ could be taken as a non-obvious upper bound of the number of variables of PIs of a.e. satisfiable formula in $\Omega(n,c,r)$. Nevertheless $(\alpha_M^r(c)+\varepsilon)n$ could be greater than the number of variables occurring in these satisfiable formulae, which is not admissible. Likewise the upper bound of the normalized length of PIs, $(\alpha_m^r(c)/(1-\mathrm{e}^{-rc}))+\varepsilon'$ (with $\varepsilon'>0$ as small as we want), could be greater than 1 which is also not admissible. However, if $\alpha_M^r(c)$ satisfies the relation: $\alpha_M^r(c)<1-\mathrm{e}^{-rc}$, this definitely guarantees obtaining a non-obvious upper bound of the normalized length. Let us examine more precisely the condition which $\alpha_M^r(c)$ must satisfy as a function of c. Let $\tilde{c}_r<1$ be such that $1-e^{-r\tilde{c}_r}=\tilde{c}_r$ ($\tilde{c}_2\simeq 0.79$, $\tilde{c}_3\simeq 0.94$, $\tilde{c}_4\simeq 0.98,\ldots$ and as $r\to\infty$, $\tilde{c}_r\to 1$). For $c<\tilde{c}_r$, we have $c<1-\mathrm{e}^{-rc}$ and if $\alpha_M^r(c)$ exists such that $\alpha_M^r(c)\leqslant c$, then we have $\alpha_M^r(c)/(1-\mathrm{e}^{-rc})<1$. For $c\geqslant\tilde{c}_r$, we have $c\geqslant 1-\mathrm{e}^{-rc}$ and if $\alpha_M^r(c)$ exists such that $\alpha_M^r(c)<\inf(1,c)$, then $\alpha_M^r(c)$ must satisfy the relation $\alpha_M^r(c)<1-\mathrm{e}^{-rc}$. In conclusion, for any $c>0$, if $\alpha_M^r(c)$ exists, then it must additionally satisfy the relation $\alpha_M^r(c)<\inf(1-\mathrm{e}^{-rc},c)$. We will show in Section 3 that for 2- and 3-CNF formulae and for any c greater than a value denoted by c_r^0 and defined as the unique positive root of the following equation:

$$-(1-c)\ln(1-c)-c+c\ln(r)+(r-1)c\ln(1-c/2)=0$$

($c_2^0\sim 0.566, c_3^0\sim 0.598$), $\alpha_M^r(c)$ exists and satisfies the relation $\alpha_M^r(c)<\inf(1-\mathrm{e}^{-rc},c)$. We will show that for r-CNF formulae, from $r=4$, the range of values where $\alpha_M^r(c)$

exists is more restrictive and even more so if the relation $\alpha_M^r(c) < \inf(1-e^{-rc}, c)$ is to be satisfied. That is to say, $\alpha_M^r(c)$ exists and satisfies the relation $\alpha_M^r(c) < \inf(1-e^{-rc}, c)$ for every $c \in [c_r^0, c_r^1[$ and for every $c > c_r^2$, c_r^1 and c_r^2 being defined as the respective lower and upper roots of the equation $f_{r,c}(1-e^{-rc}) = 1$ ($\{c_4^1 \sim 4.358, c_4^2 \sim 9.365\}, \{c_5^1 \sim 6.097, c_5^2 \sim 20.678\}, \ldots$). It appears from experiments that c_r^2 is slightly lower than the estimate value of the supposed threshold [5]. The theorems corresponding to these results are as follows:

Theorem 1.4 (Upper bound). *For $r = 2, 3$, for any $\varepsilon > 0$ and for every $c \geqslant c_r^0$, almost every formula in $\Omega(n, c, r)$:*

- *either is satisfiable and any one of its prime implicants has a normalized length lower than $(\alpha_M^r(c)/(1-e^{-rc})) + \varepsilon$, where $\alpha_M^r(c)$ is the upper root of $f_{r,c}(\alpha) = 1$ and $\alpha_M^r(c)/(1-e^{-rc}) < 1$,*
- *or is unsatisfiable.*

Theorem 1.5 (Upper bound). *For $r \geqslant 4$, for any $\varepsilon > 0$ and for every $c \in]c_r^0, c_r^1[\cup]c_r^2, +\infty[$ c_r^1 and c_r^2 being the lower and upper roots, respectively, of $f_{r,c}(1-e^{-rc}) = 1$, almost every formula in $\Omega(n, c, r)$:*

- *either is satisfiable and any one of its prime implicants has a normalized length lower than $(\alpha_M^r(c)/(1-e^{-rc})) + \varepsilon$, where $\alpha_M^r(c)$ is the upper root of $f_{r,c}(\alpha) = 1$ and $\alpha_M^r(c)/(1-e^{-rc}) < 1$,*
- *or is unsatisfiable.*

As a direct consequence of these theorems we can derive an exponential lower bound on the actual number of solutions of a.e. satisfiable formula in $\Omega(n, c, r)$. Let us call the variables not occurring in a PI $\mathcal{I}$ of a formula Φ, *free variables* with respect to $\mathcal{I}$. The truth assignments to the variables of Φ such that the literals of $\mathcal{I}$ take the value 1 and the free variables with respect to $\mathcal{I}$ any value 0 or 1, satisfy Φ. Thus from the upper bound of the normalized lengths of PIs provided by the preceding theorems, we can derive an exponential lower bound for the actual number of solutions of a.e. satisfiable formula in $\Omega(n, c, r)$, namely $2^{(1-e^{-rc}-\alpha_M^r(c)-\varepsilon)n}$. Moreover, for 2- and 3-CNF formulae, we will show that all the $\alpha_M^r(c)$ have a maximum strictly smaller than 1. This allows us to give an exponential lower bound independent of c. The statements of those results are:

Theorem 1.6. *For $r = 2, 3$, for any $\varepsilon > 0$ and for every $c > c_r^0$, almost every formula in $\Omega(n, c, r)$:*

- *either is satisfiable and has an exponential actual number of solutions which is at least equal to $2^{(1-e^{-rc}-\alpha_M^r(c)-\varepsilon)n}$, and (irrespective of c) greater than $2^{0.03n}$ if $r = 2$, or $2^{0.012n}$ if $r = 3$,*
- *or is unsatisfiable.*

Theorem 1.7. *For $r \geqslant 4$, for any $\varepsilon > 0$ and for every $c \in]c_r^0, c_r^1[\cup]c_r^2, +\infty[$, almost every formula in $\Omega(n, c, r)$:*

- *either is satisfiable and has an exponential actual number of solutions which is at least equal to* $2^{(1-e^{-rc}-\alpha_M^r(c)-\varepsilon)n}$,
- *or is unsatisfiable.*

From those exponential lower bounds, one can note that for each value of c lower than and close to the supposed (or demonstrated for $r=2$) threshold, the solutions of a.e. satisfiable formula in $\Omega(n,c,r)$ are not extremely rare. From experiments this might seem unexpected since, as the ratio c approaches the threshold, the difficulty of solving satisfiable formulae increases very strongly and seems to be maximum at the threshold. This could suggest that solutions become extremely rare in a small neighbourhood at the left of the threshold.

The layout of this paper is as follows. In the next section we calculate the expectation of the number of PIs of a random formula of $\Omega(n,c,r)$ as a function of their length and we derive the exponential order of the expectation given by Proposition 1.2. We establish some properties of the base $f_{r,c}(\alpha)$ of this exponential order, in particular, that $f_{r,c}(\alpha)$ is unimodal. In section 3 we prove first Theorems 1.3, 1.4, 1.6 concerning 2 and 3-CNF formulae and then we extend Theorem 1.3 to r-CNF formulae with $r\geqslant 4$ and we prove Theorems 1.5 and 1.7 concerning these formulae. For $r=2,3,4,5$ and for some values of c, we list the corresponding values of $\alpha_m^r(c)/(1-e^{-rc}), \alpha_M^r(c)/(1-e^{-rc})$ and $2^{(1-e^{-rc}-\alpha_M^r(c)-\varepsilon)n}$.

2. Expectation of the number of prime implicants

2.1. Definitions

We give some specific definitions concerning ordinary and prime implicants of CNF formulae. In all the following definitions, F refers to a CNF formula over a set X of n boolean variables. We will say that a set of literals is consistent iff it contains no pair of opposite literals, i.e. x and $\neg x$.

Definition 2.1. Given a consistent set of literals I over X, a clause C of F is an I_s-clause iff C contains exactly s distinct literals of I.

Example.

$$F \equiv C_1 \wedge C_2 \wedge C_3 \wedge C_4$$

with

$$C_1 \equiv a \vee \neg b \vee \neg c, \quad C_2 \equiv a \vee b \vee \neg c, \quad C_3 \equiv \neg a \vee b \vee \neg c, \quad C_4 \equiv \neg a \vee b \vee c.$$

Let: $I=\{\neg a, b, c\}$, then C_1 is an I_0-clause, C_2 an I_1-clause, C_3 an I_2-clause and C_4 an I_3-clause.

Definition 2.2. A consistent set I of literals over X is an implicant of F iff F does not contain any I_0-clause.

A consequence of the above definition is that under the truth assignment to the variables of an Implicant I of F such that every literal of I takes the value 1, every clause of F has the value 1 and therefore F also has the value 1. This fits with the classical definition of an Implicant. In the previous example, I is not an Implicant since C_1 is an I_0-clause.

Definition 2.3. An Implicant I of F is called a prime implicant (PI for short) iff for any literal $l \in I$, $I - \{l\}$ is not an Implicant of F.

We call length of a PI I of F, the number p of its literals with $0 \leqslant p \leqslant n$. Any variable of X which does not appear in I is called a *free variable* with respect to I. A solution of F can be obtained from I by assigning the truth values to the variables of I such that every literal of I takes the value 1 and by assigning any truth value 0 or 1 to the free variables with respect to I. By this way from a PI I of F having p literals we can obtain 2^{n-p} solutions of F (but the actual number of solutions may be lower).

The condition for a consistent set of literals over X to be a PI of F can be expressed simply with respect to some clauses of F. For any literal l of a PI of F there must exist at least a clause of F which is satisfied uniquely by l. This necessary and sufficient condition is expressed by the following proposition:

Proposition 2.1. *An implicant I of F is a prime implicant iff every literal $l \in I$ appears in at least an I_1-clause of F.*

Proof. Assume that I is an implicant such that there is at least a literal l which does not appear in any I_1-clause. Consider the set $I' = I - \{l\}$, the I_s-clauses where l appears, are I'_{s-1}-clauses. Since l appears in no I_1-clause then the I'_s-clauses are such that $s > 0$ and I' is therefore an implicant. Then, I is not a prime implicant.

Conversely assume that I is an implicant such that every $l \in I$ appears in at least an I_1-clause, say $C(l)$. For $I' = I - \{l\}$, $C(l)$ is an I'_0-clause and then I' is not an implicant. Consequently I is a prime implicant. □

Example.

$$F \equiv C_1 \wedge C_2 \wedge C_3,$$

where

$$C_1 \equiv a \vee \neg b \vee \neg c, \qquad C_2 \equiv a \vee b \vee \neg c, \qquad C_3 \equiv \neg a \vee b \vee c$$

$I = \{a, b\}$ is a PI of F since there is no I_0-clause in F and a and b appear in the I_1-clauses C_1 and C_3 respectively.

Definition 2.4. The normalized length of a prime implicant of F is the ratio of the number of its literals to the actual number of variables of F.

In the above example the normalized length of $I = \{a, b\}$ is 2/3.

2.2. The expected number of prime implicants of a random formula of $\Omega(n,c,r)$ as a function of their length

In this subsection we calculate the expectation of the number of PIs with a fixed length $p \geqslant 0$ of a random formula of $\Omega(n,c,r)$. From now on, we assume that $n \geqslant r \geqslant 2$.

We consider first the general case $c>0$ and $p \geqslant 1$ and later the special cases where $c=0$ and/or $p=0$.

Assume $c>0$ and $p \geqslant 1$. We calculate first the probability that a fixed consistent set of p literals denoted by I^p is a PI of a random formula of $\Omega(n,c,r)$. We denote this probability by $\mathbf{Pr}(I^p)$. For this we compute the number of formulae of $\Omega(n,c,r)$ such that I^p is a PI divided by the number of formulae in $\Omega(n,c,r)$. Notice that from the definition of $\Omega(n,c,r)$, an r-CNF formula of $\Omega(n,c,r)$ is an ordered conjunction of clauses. For each formula of $\Omega(n,c,r)$ such that I^p is a PI, the set of clauses can be partitioned into two disjoint subsets: the set of I_1^p-clauses and the set of I_s^p-clauses with $s=2,\ldots,r$. Let us denote by q the cardinal of the set of I_1^p-clauses of a formula in $\Omega(n,c,r)$ such that I^p is a PI. By proposition 2.1, q satisfies the relation $p \leqslant q \leqslant c\,n$. Every formula of $\Omega(n,c,r)$ such that I^p is a PI and having q I_1^p-clauses can be obtained as follows.

(a) Choose q integers in $\{1,\ldots,cn\}$ which will be the ranks of the q I_1^p-clauses in the conjunction of cn clauses to be built up. There are $\binom{cn}{q}$ possible choices of these q ranks. Let R be the set of the q chosen ranks.

(b) Partition R into p non-empty subsets. $S(q,p)$ denoting the Stirling number of the second kind, there are $S(q,p)$ partitions of R into p non-empty subsets.

(c) Map in a one-to-one correspondence the p literals of I^p to the p subsets of the preceding partition of R. There are $p!$ such mappings.
For every rank ρ of R, choose an I_1^p-clause which contains the literal of I^p associated by the preceding one-to-one correspondence, with the subset of the partition to which ρ belongs. Apart from one literal of every I_1^p-clause which is fixed, the other literals of an I_1^p-clause can be negations of literals of I^p and literals associated with the free variables with respect to I^p. Let j be the number of free variables appearing in an I_1^p-clause. The number of such possible I_1^p-clauses containing a fixed literal of I^p is

$$u_r(p,n)=\sum_{j=0}^{r-1} 2^j \binom{n-p}{j}\binom{p-1}{r-1-j} \tag{2.1}$$

with the convention that if $a<b$ then $\binom{a}{b}=0$. There are therefore $(u_r(p,n))^q$ choices of q I_1^p-clauses in the conditions mentioned above for the q ranks in R.

(d) There remain to be chosen $(cn-q)$ I_s^p-clauses with $2 \leqslant s \leqslant r$, to be placed at the ranks $\{1,\ldots,cn\}\backslash R$, in order to form with the I_1^p clauses placed at the ranks of R, the desired ordered conjunction of cn clauses. An I_s^p-clause must contain s literals of I^p and r-s literals which can be either negations of literals of I^p, or literals associated with free variables with respect to I^p. Let j be the number of free variables appearing in an I_s^p-clause. They are $2^j\binom{n-p}{j}\binom{p-s}{r-s-j}$ possible I_s^p-clauses

containing s literals of I^p, j literals associated with free variables and $r-s-j$ negations of literals of I^p. Hence there are:

$$v_r(p,n)=\sum_{s=2}^{r}\sum_{j=0}^{r-s}\binom{p}{i}2^j\binom{n-p}{j}\binom{p-s}{r-s-j} \tag{2.2}$$

possible I_s^p-clauses with $s=2,\ldots,r$. Again with the convention mentioned above (if $a<b$ then $\binom{a}{b}=0$), the number of choices of $(cn-q)$ I_s^p-clauses with $s=2,\ldots,r$, at ranks $\{1,\ldots,cn\}\backslash R$ is therefore $(v_r(p,n))^{(cn-q)}$.

It follows from what precedes that the number of distinct formulae of $\Omega(n,c,r)$ such that I^p is a PI and having $q=p,\ldots,cn$ I_1^p-clauses is

$$\sum_{q=p}^{cn}\binom{cn}{q}S(q,p)\,p!\,(u_r(p,n))^q\,(v_r(p,n))^{cn-q}.$$

The total number of possible clauses with r distinct literals over n variables being $W_r=2^r\binom{n}{r}$ and thereby the total number of formulae of $\Omega(n,c,r)$ being $(W_r)^{cn}$, we have

$$\mathbf{Pr}(I^p)=\frac{1}{(W_r)^{cn}}\sum_{q=p}^{cn}\binom{cn}{q}S(q,p)\,p!\,(u_r(p,n))^q\,(v_r(p,n))^{cn-q}.$$

There are $2^p\binom{n}{p}$ distinct consistent sets of literals over n variables which can be PIs of length p of a formula in $\Omega(n,c,r)$. We denote by $\mathscr{PI}^p_{r,c,n}$ the set of PIs, with length p, of a random formula in $\Omega(n,c,r)$. Thus, the mathematical expectation of $|\mathscr{PI}^p_{r,c,n}|$ is

$$\begin{aligned}\mathbf{E}(|\mathscr{PI}^p_{r,c,n}|)&=2^p\binom{n}{p}\mathbf{Pr}(I^p)\\&=2^p\binom{n}{p}\frac{1}{(W_r)^{cn}}\sum_{q=p}^{cn}g\binom{cn}{q}S(q,p)\,p!\,(u_r(p,n))^q\,(v_r(p,n))^{cn-q}.\end{aligned} \tag{2.3}$$

We now examine the special cases.

(1) $p=0$ with $c>0$. There is no formula in $\Omega(n,c,r)$ such that $c>0$ and I^0 is a PI, hence $\mathbf{E}(|\mathscr{PI}^0_{r,c,n}|)=0$.

(2) $p\geqslant 1$ with $c=0$. There is no PI of length $p\geqslant 1$ which implies that formula, hence $\mathbf{E}(|\mathscr{PI}^p_{r,0,n}|)=0$.

(3) $p=0$ with $c=0$. By convention we say that I^0 logically implies the empty formula and then $\mathbf{E}(|\mathscr{PI}^0_{r,0,n}|)=1$.

With the conventions that if $b>a$ then $\binom{a}{b}=0$ and $S(a,b)=0$, that $\binom{0}{0}=1$ and that $S(0,0)=0$, relation (2.3) holds for the special cases (1)–(3). We can therefore state:

Proposition 2.2. *The expected number of prime implicants with length p of a random formula of $\Omega(n,c,r)$ is*

$$\begin{aligned}\mathbf{E}(|\mathscr{PI}^p_{r,c,n}|)&=2^p\binom{n}{p}\mathbf{Pr}(I^p)\\&=2^p\binom{n}{p}\frac{1}{(W_r)^{cn}}\sum_{q=p}^{cn}\binom{cn}{q}S(q,p)\,p!(u_r(p,n))^q\,(v_r(p,n))^{cn-q}.\end{aligned}$$

Denoting by $\mathscr{PI}^{\alpha n}_{r,c,n}$ the set of all prime implicants of a random formula of $\Omega(n,c,r)$, we derive from Proposition 2.2 that the expectation of the total number of PIs is, for $c>0$:

$$\mathbf{E}(|\mathscr{PI}_{r,c,n}|)=\sum_{p=1}^{n}\mathbf{E}(|\mathscr{PI}^{p}_{r,c,n}|)$$

and for $c=0$:

$$\mathbf{E}(|\mathscr{PI}_{r,0,n}|)=1.$$

2.3. The exponential order of the expected number of prime implicants

In this subsection we provide first the exponential order of the expected number of PIs of a random formula of $\Omega(n,c,r)$, as a function of their length. We show that this exponential order is unimodal as a function of the length of PIs and we establish some other properties.

To calculate the exponential order, we need first to establish estimates from below and from above of the expectation.

Let $\alpha=p/n$, $\beta=q/(cn)$. From now on we assume c,α and β to be non-zero rationals such that $\alpha\in]0,\inf(1,c)]$, $\beta\in]0,1]$ and satisfying the relation $\beta c\geqslant\alpha$. We rewrite $\mathbf{E}(|\mathscr{PI}^{p}_{r,c,n}|)$ (Proposition 2.2) as a function of α and β:

$$\mathbf{E}(|\mathscr{PI}^{\alpha n}_{r,c,n}|)=2^{p}\binom{n}{\alpha n}\frac{1}{(W_r)^{cn}}\sum_{\beta=\frac{\alpha n}{cn},\frac{\alpha n+1}{cn},\ldots,\frac{cn-1}{cn},1}\binom{cn}{\beta cn}$$
$$\times S(\beta c n,\alpha n)(\alpha n)!(u_r(\alpha n,n))^{\beta cn}(v_r(\alpha n,n))^{(1-\beta)cn}. \tag{2.4}$$

Proposition 2.3. *We have*

$$\sum_{\beta=\frac{\alpha n}{cn},\frac{\alpha n+1}{cn},\ldots,\frac{cn-1}{cn},1}\mu_{r,c}(\alpha,\beta,n)(\mathscr{F}^{\alpha}_{r,c,n}(\beta))^{n}\leqslant\mathbf{E}(|\mathscr{PI}^{\alpha n}_{r,c,n}|)$$
$$\leqslant\sum_{\beta=\frac{\alpha n}{cn},\frac{\alpha n+1}{cn},\ldots,\frac{cn-1}{cn},1}\nu_{r,c}(\alpha,\beta,n)(\mathscr{F}^{\alpha}_{r,c}(\beta))^{n} \tag{2.5}$$

with

$$\mathscr{F}^{\alpha}_{r,c,n}(\beta)=(1-\alpha)^{-(1-\alpha)}\left(\frac{2(\mathrm{e}^{x_0}-1)}{\alpha}\right)^{\alpha}\left(\frac{(1-\beta)c\,\kappa_{r,n}(\alpha)}{e\,x_0\,\zeta_{r,n}(\alpha)}\right)^{\beta c}\left(\frac{\zeta_{r,n}(\alpha)}{(1-\beta)\,\phi_r}\right)^{c},$$

$$\mathscr{F}^{\alpha}_{r,c}(\beta)=(1-\alpha)^{-(1-\alpha)}\left(\frac{2(\mathrm{e}^{x_0}-1)}{\alpha}\right)^{\alpha}\left(\frac{(1-\beta)c\,\kappa_{r}(\alpha)}{e\,x_0\,\zeta_{r}(\alpha)}\right)^{\beta c}\left(\frac{\zeta_{r}(\alpha)}{(1-\beta)\,\phi_r}\right)^{c},$$

x_0 being the unique positive root of the equation below if $\beta>\alpha/c$, or the unique root 0 if $\beta=\alpha/c$:

$$1-\mathrm{e}^{-x}-\frac{\alpha}{\beta c}x=0 \tag{2.6}$$

and

$$\kappa_{r,n}(\alpha)=\frac{(2-\alpha-\frac{1}{n})^{r-1}}{(r-1)!},\qquad \kappa_r(\alpha)=\frac{(2-\alpha)^{r-1}}{(r-1)!},$$

$$\zeta_{r,n}(\alpha)=\frac{1}{r!}\left[\left(2-\frac{r}{n}\right)^r-\left(2-\alpha-\frac{r}{n}\right)^r-\alpha r\left(2-\alpha-\frac{r}{n}\right)^{r-1}\right],$$

$$\zeta_r(\alpha)=\frac{1}{r!}[2^r-(2-\alpha)^r-\alpha r(2-\alpha)^{r-1}],$$

$$\phi_r=\frac{2^r}{r!},$$

$$\nu_{r,c}(\alpha,\beta,n)=\left(1-\frac{r-1}{n}\right)^{-(r-1)cn}\sqrt{2\pi\alpha n}e^{1/(12\alpha n)}[1+\varepsilon(\beta cn,\alpha n)]. \tag{2.7}$$

For $\alpha\neq 1$:

$$\mu_{r,c}(\alpha,\beta,n)=\left(1-\inf\left(1,\frac{r}{(1-\alpha)n}\right)\right)^{crn}\left(1-\inf\left(1,\frac{r}{\alpha n}\right)\right)^{(2-\beta)crn}$$
$$\times\frac{2}{\pi cn}\sqrt{\frac{2\alpha}{\beta e}}\,e^{1/(12\alpha n+1)}[1+\varepsilon(\beta cn,\alpha n)]. \tag{2.8}$$

For $\alpha=1$:

$$\mu_{r,c}(1,\beta,n)=\left(1-\inf\left(1,\frac{r}{n}\right)\right)^{(2-\beta)crn}\frac{2}{\pi cn}\sqrt{\frac{2}{\beta e}}e^{1/(12n+1)}[1+\varepsilon(\beta cn,n)] \tag{2.9}$$

with $\varepsilon(\beta cn,\alpha n)\to 0$ *as* $\beta c n\to\infty$ *regardless of the relation of* αn *to* βcn.

Proof. Using classical upper and lower bounds for the binomial coefficient we can write the following inequalities for $\binom{n}{\alpha n}$ and $\binom{cn}{\beta cn}$ in the expression of $\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c,n}|)$ (2.4):

$$\sqrt{2/(\pi n)}\,e^{-1/6}\alpha^{-\alpha n}(1-\alpha)^{-(1-\alpha)n}\leqslant\binom{n}{\alpha n}\leqslant\alpha^{-\alpha n}(1-\alpha)^{-(1-\alpha)n}, \tag{2.10}$$

$$\sqrt{2/(\pi cn)}e^{-1/6}\beta^{-\beta cn}(1-\beta)^{-(1-\beta)cn}\leqslant\binom{cn}{\beta cn}\leqslant\beta^{-\beta cn}(1-\beta)^{-(1-\beta)cn}. \tag{2.11}$$

For the factor W_r of $\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c,n}|)$ in (2.4) we can write

$$\frac{r!}{2^r n^r}\leqslant\frac{1}{W_r}\leqslant\frac{r!}{2^r n^r}\left(1-\frac{r-1}{n}\right)^{-(r-1)}. \tag{2.12}$$

Using an approximation of the Stirling number of the second kind established by Temme in [23] and transforming it as in [6] we can write the following inequality for

$S(\beta cn, \alpha n)$ of $\mathbf{E}(|\mathscr{P}.\mathscr{I}^{\alpha n}_{r,c,n}|)$ (2.4):

$$x_0^{-\beta cn}(e^{x_0}-1)^{\alpha n}e^{-(\beta c-\alpha)n}(\beta cn)^{\beta cn}(\alpha n)^{-(\alpha n)}(\pi\beta cn)^{-1/2}e^{-1/6}[1+\varepsilon(\beta cn,\alpha n)]$$
$$\leqslant S(\beta cn,\alpha n)\leqslant x_0^{-\beta cn}(e^{x_0}-1)^{\alpha n}e^{-(\beta c-\alpha)n}(\beta cn)^{(\beta cn)}(\alpha n)^{-(\alpha n)}[1+\varepsilon(\beta cn,\alpha n)] \tag{2.13}$$

with x_0 the positive root of the equation below if $\beta c > \alpha$ or the unique root 0 if $\beta c = \alpha$:

$$1-e^{-x}-\frac{\alpha}{\beta c}x=0$$

and $\varepsilon(\beta cn, \alpha n) \to 0$ as $\beta cn \to \infty$ regardless of the relation of αn to βcn. Using Stirling's formula we have

$$(\alpha n)^{\alpha n}e^{-\alpha n}\sqrt{2\pi\alpha n}\,e^{1/(12\alpha n+1)}\leqslant(\alpha n)!\leqslant(\alpha n)^{\alpha n}e^{-\alpha n}\sqrt{2\pi\alpha n}\,e^{1/12\alpha n}. \tag{2.14}$$

Finally, for $\alpha \neq 1$ the following inequalities for $u_r(\alpha n, n)$ (2.1) and $v_r(\alpha n, n)$ (2.2) can be easily obtained:

$$\left(1-\inf\left(1,\frac{r}{(1-\alpha)n}\right)\right)^r\left(1-\inf\left(1,\frac{r}{\alpha n}\right)\right)^r\kappa_{r,n}(\alpha)n^{r-1}\leqslant u_r(\alpha n,n)\leqslant\kappa_r(\alpha)n^{r-1}, \tag{2.15}$$

where

$$\kappa_{r,n}(\alpha)=\frac{(2-\alpha-\frac{1}{n})^{r-1}}{(r-1)!},\qquad \kappa_r(\alpha)=\frac{(2-\alpha)^{r-1}}{(r-1)!}$$

and

$$\left(1-\inf\left(1,\frac{r}{(1-\alpha)n}\right)\right)^r\left(1-\inf\left(1,\frac{r}{\alpha n}\right)\right)^{2r}\zeta_{r,n}(\alpha)n^r\leqslant v_r(\alpha n,n)\leqslant\zeta_r(\alpha)n^r \tag{2.16}$$

with

$$\zeta_{r,n}(\alpha)=\frac{1}{r!}\left[\left(2-\frac{r}{n}\right)^r-\left(2-\alpha-\frac{r}{n}\right)^r-\alpha r\left(2-\alpha-\frac{r}{n}\right)^{r-1}\right],$$

$$\zeta_r(\alpha)=\frac{1}{r!}[2^r-(2-\alpha)^r-\alpha r(2-\alpha)^{r-1}].$$

For $\alpha = 1$ inequalities (2.15) and (2.16) are obviously to be replaced by

$$\left(1-\inf\left(1,\frac{r}{n}\right)\right)^r\kappa_{r,n}(1)n^{r-1}\leqslant u_r(n,n)\leqslant\kappa_r(1)n^{r-1} \tag{2.17}$$

and

$$\left(1-\inf\left(1,\frac{r}{n}\right)\right)^{2r}\zeta_{r,n}(1)n^r\leqslant v_r(n,n)\leqslant\zeta_r(1)n^r. \tag{2.18}$$

Combining inequalities (2.10)–(2.14), and if $\alpha \neq 1$ (2.15) and (2.16) or if $\alpha = 1$ (2.17) and (2.18), we obtain the desired estimates. □

The exponential order of $\mathbf{E}(|\mathscr{P}\mathscr{I}^{\mathscr{X}n}_{r,c,n}|)$ is derived from the estimates of the preceding proposition by looking for the maximum term in the sums of (2.5). For this we show that:

Proposition 2.4. *$\mathscr{F}^{\alpha}_{r,c,n}(\beta)$ [resp. $\mathscr{F}^{\alpha}_{r,c}(\beta)$] attains an absolute maximum on $[\alpha/c, 1]$ at*

$$\beta_n^* = 1 - \frac{x_0^* \zeta_{r,n}(\alpha)}{c\kappa_{r,n}(\alpha)} \quad \left[resp.\ \beta^* = 1 - \frac{x_0^* \zeta_r(\alpha)}{c\kappa_r(\alpha)} \right]$$

with x_0^* the unique positive root of the following equation if $c > \alpha$, or the unique root 0 if

$$c = \alpha\colon\ 1 - \mathrm{e}^{-x_0} - \frac{\alpha x_0}{c - x_0 \frac{\zeta_{r,n}(\alpha)}{\kappa_{r,n}(\alpha)}} = 0 \quad \left[resp.\ 1 - \mathrm{e}^{-x_0} - \frac{\alpha x_0}{c - x_0 \frac{\zeta_r(\alpha)}{\kappa_r(\alpha)}} = 0 \right].$$

Proof. The calculation is made only for $\mathscr{F}^{\alpha}_{r,c,n}(\beta)$. The calculation for $\mathscr{F}^{\alpha}_{r,c}(\beta)$ is similar, substituting the corresponding expressions. Let:

$$\ln \mathscr{F}^{\alpha}_{r,c,n}(\beta) = -(1-\alpha)\ln(1-\alpha) + \alpha \ln\left(\frac{2(\mathrm{e}^{x_0} - 1)}{\alpha}\right) + \beta c \ln\left(\frac{(1-\beta)c\kappa_{r,n}(\alpha)}{x_0 \zeta_{r,n}(\alpha)\mathrm{e}}\right) + c \ln\left(\frac{\zeta_{r,n}(\alpha)}{(1-\beta)\phi_r}\right)$$

x_0 can be regarded as an implicit function of $\beta \in [\alpha/c, 1]$ defined by (2.6):

$$1 - \mathrm{e}^{-x_0} - \frac{\alpha}{\beta c} x_0 = 0. \tag{2.19}$$

This implicit function is clearly continuous on $]\alpha/c, 1]$. As $\beta \to \alpha/c$, $x_0 = 2(1 - \alpha/\beta c) + \mathrm{O}[(1 - \alpha/\beta c)^2]$. Hence x_0 is continuous at $\beta = \alpha/c$ and therefore on $[\alpha/c, 1]$. It follows easily that $\ln \mathscr{F}^{\alpha}_{r,c,n}(\beta)$ is continuous on $[\alpha/c, 1]$.

Assume that $c > \alpha$. The derivative of $\ln \mathscr{F}^{\alpha}_{r,c,n}(\beta)$, allowing for (2.19), is

$$\frac{\mathrm{d} \ln \mathscr{F}^{\alpha}_{r,c,n}(\beta)}{\mathrm{d}\beta} = c \ln\left(\frac{(1-\beta)c\kappa_{r,n}(\alpha)}{x_0 \zeta_{r,n}(\alpha)}\right).$$

$\mathrm{d} \ln \mathscr{F}^{\alpha}_{r,c,n}(\beta)/\mathrm{d}\beta$ is continuous on $]\alpha/c, 1[$. For any $\beta \in]\alpha/c, 1[$, let $\beta_n^* = 1 - x_0 \zeta_{r,n}(\alpha)/c\kappa_{r,n}(\alpha)$ (x_0 depends on β by (2.19)). Consider the equation obtained from Eq. (2.19) by substituting β_n^* for β:

$$1 - \mathrm{e}^{-x_0} - \frac{\alpha x_0}{c - x_0 \frac{\zeta_{r,n}(\alpha)}{\kappa_{r,n}(\alpha)}} = 0. \tag{2.20}$$

It can be easily shown that for any $c > 0$ and any $\alpha \in]0, \inf(1, c)[$ or $\alpha = 1 \neq c$, (2.20) has a unique positive root. We denote it by x_0^*. The couple (x_0^*, β_n^*) satisfies (2.19), and so we have $(\mathrm{d} \ln \mathscr{F}^{\alpha}_{r,c,n}/\mathrm{d}\beta)(\beta_n^*) = 0$. By the unicity of x_0^* for given c and α, β_n^* is the unique value of β on $]\alpha/c, 1[$ such that $(\mathrm{d} \ln \mathscr{F}^{\alpha}_{r,c,n}/\mathrm{d}\beta)(\beta) = 0$. Thus on $]\alpha/c, 1[$, $(\mathrm{d} \ln$

$\mathscr{F}^{\alpha}_{r,c,n}/\mathrm{d}\beta)(\beta)$ changes sign only once, namely at $\beta=\beta^*_n$. As $\beta\to\alpha/c$, $(\mathrm{d}\ln\mathscr{F}^{\alpha}_{r,c,n}/\mathrm{d}\beta)(\beta)\to+\infty$ and as $\beta\to 1$, $(\mathrm{d}\ln\mathscr{F}^{\alpha}_{r,c,n}/\mathrm{d}\beta)(\beta)\to-\infty$. We can then conclude that $\ln\mathscr{F}^{\alpha}_{r,c,n}(\beta)$ increases on $]\alpha/c,\beta^*_n[$, attains an absolute maximum at $\beta=\beta^*_n$, then decreases on $]\beta^*_n,1[$. By continuity of $\ln\mathscr{F}^{\alpha}_{r,c,n}(\beta)$ at $\beta=\alpha/c$ and $\beta=1$, $\ln\mathscr{F}^{\alpha}_{r,c,n}(\beta^*_n)$ is an absolute maximum on $[\alpha/c,1]$.

Now we examine the special case $c=\alpha$. Since $\beta\in[\alpha/c,1]$, β can only take the value 1. The maximum point of $\ln\mathscr{F}^{\alpha}_{r,c,n}(\beta)$ is therefore obviously $\beta=1$. From Eq. (2.20) we observe that as $\alpha\to c\leqslant 1$, $x^*_0\leqslant 2(1-\alpha/c)+\mathrm{O}[(1-\alpha/c)^2]$ and therefore tends to 0. Thus for $\alpha=c$, $\beta^*_n=1$ which is the correct maximum point. □

We can now easily prove Proposition 1.2.

Proof of Proposition 1.2. By Proposition 2.3 we can derive from (2.5):

$$\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c,n}|)\leqslant(\mathscr{F}^{\alpha}_{r,c}(\beta^*))^n\sum_{\beta=\frac{\alpha n}{cn},\frac{\alpha n+1}{cn},\ldots,\frac{cn-1}{cn},1}v_{r,c}(\alpha,\beta,n).$$

By (2.7), for n sufficiently large we have

$$v_{r,c}(\alpha,\beta,n)\leqslant 2\left(1-\frac{r-1}{n}\right)^{-(r-1)cn}\sqrt{2\pi\alpha n}\,\mathrm{e}^{1/(12\alpha n)}$$

and then

$$\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c,n}|)\leqslant 2cn\left(1-\frac{r-1}{n}\right)^{-(r-1)cn}\sqrt{2\pi\alpha n}(\mathscr{F}^{\alpha}_{r,c}(\beta^*))^n\mathrm{e}^{1/(12\alpha n)}. \tag{2.21}$$

We deduce

$$\lim_{n\to\infty}\sup[\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c,n}|)]^{1/n}\leqslant\mathscr{F}^{\alpha}_{r,c}(\beta^*). \tag{2.22}$$

We show now that we can bound from below the lower limit of $[\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|)]^{1/n}$ also by $\mathscr{F}^{\alpha}_{r,c}(\beta^*)$. Since $\lim_{n\to\infty}\mathscr{F}^{\alpha}_{r,c,n}(\beta^*_n)=\mathscr{F}^{\alpha}_{r,c}(\beta^*)$, for any $\eta/2>0$ there is a number $N_1(\eta)$ such that for every $n>N_1(\eta)$ we have $\mathscr{F}^{\alpha}_{r,c,n}(\beta^*)-\eta/2\leqslant\mathscr{F}^{\alpha}_{r,c,n}(\beta^*_n)$. $\mathscr{F}^{\alpha}_{r,c,n}(\beta)$ being continuous at β^*_n, for any $\eta/2>0$ there exists $\delta(\eta)>0$ such that for all $\beta\in[\alpha/c,1]$, $|\beta-\beta^*_n|<\delta(\eta)\Rightarrow\mathscr{F}^{\alpha}_{r,c,n}(\beta^*_n)-\eta/2<\mathscr{F}^{\alpha}_{r,c,n}(\beta)$. Moreover, there exists $N_2(\eta)$ such that for every $n>N_2(\eta)$, $]\beta^*_n-\delta(\eta),\beta^*_n+\delta(\eta)[\cap[\alpha n/cn,(\alpha n+1)/cn,\ldots,(cn-1)/cn,1]\neq\emptyset$. Consequently, for any $\eta>0$ and every $n>\sup(N_1(\eta),N_2(\eta))$ there exists $\widetilde{\beta}_n\in[\alpha n/cn,(\alpha n+1)/c\,n,\ldots,(cn-1)/cn,1]$ such that

$$\begin{aligned}\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|)&\geqslant\mu_{r,c}(\alpha,\widetilde{\beta}_n,n)(\mathscr{F}^{\alpha}_{r,c}(\widetilde{\beta}_n))^n\geqslant\mu_{r,c}(\alpha,\widetilde{\beta}_n,n)(\mathscr{F}^{\alpha}_{r,c}(\beta^*_n)-\eta/2)^n\\&\geqslant\mu_{r,c}(\alpha,\widetilde{\beta}_n,n)(\mathscr{F}^{\alpha}_{r,c}(\beta^*)-\eta)^n.\end{aligned} \tag{2.23}$$

$\mu_{r,c}(\alpha,\widetilde{\beta}_n,n)$ can be bounded from below for $\alpha\neq 1$:

$$\begin{aligned}\mu_{r,c}(\alpha,\widetilde{\beta}_n,n)\geqslant&\left(1-\inf\left(1,\frac{r}{(1-\alpha)n}\right)\right)^{crn}\left(1-\inf\left(1,\frac{r}{\alpha n}\right)\right)^{2crn}\frac{2}{\pi cn}\sqrt{\frac{2\alpha}{\mathrm{e}}}\\&\times\mathrm{e}^{1/(12\alpha n+1)}[1+\varepsilon(\widetilde{\beta}_n cn,\alpha n)]\end{aligned} \tag{2.24}$$

and for $\alpha = 1$:

$$\mu_{r,c}(1,\widetilde{\beta}_n,n) \geqslant \left(1 - \inf\left(1,\frac{r}{n}\right)\right)^{2crn} \frac{2}{\pi cn}\sqrt{\frac{2}{e}}\, e^{1/(12n+1)}[1 + \varepsilon(\widetilde{\beta}_n cn, n)]. \tag{2.25}$$

Since $\alpha/c \leqslant \widetilde{\beta}_n \leqslant 1$, as $n \to \infty$, $\widetilde{\beta}_n c\, n \to \infty$ and then $\varepsilon(\widetilde{\beta}_n c\, n, n) \to 0$. From (2.24) and (2.25) we conclude that for $\alpha \in]0, \inf(1,c)[$:

$$1 \leqslant \lim_{n\to\infty} \inf[\mu_{r,c}(\alpha,\widetilde{\beta}_n,n)]^{1/n}. \tag{2.26}$$

From this latter limit and from (2.23) we deduce that for any $\eta > 0$:

$$\mathscr{F}^{\alpha}_{r,c}(\beta^*) - \eta \leqslant \lim_{n\to\infty} \inf[\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|)]^{1/n}.$$

Consequently,

$$\mathscr{F}^{\alpha}_{r,c}(\beta^*) \leqslant \lim_{n\to\infty} \inf[\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|)]^{1/n}. \tag{2.27}$$

Finally, by (2.22) and (2.27), we have

$$\lim_{n\to\infty} [\mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|)]^{1/n} = \mathscr{F}^{\alpha}_{r,c}(\beta^*).$$

Putting

$$f_{r,c}(\alpha) = \mathscr{F}^{\alpha}_{r,c}(\beta^*) = (1-\alpha)^{-(1-\alpha)} \left(\frac{2(e^{x_0^*} - 1)}{\alpha}\right)^{\alpha} e^{(\zeta_r(\alpha)/\kappa_r(\alpha))x_0^* - c} \left(\frac{c\,\kappa_r(\alpha)}{x_0^*\phi_r}\right)^{c}$$

and renaming x_0^* and x_0 by x_0 and x respectively we obtain the statement of Proposition 1.2. □

It can be noted that the exponential order $f_{r,c}(\alpha)$ tends to the expectation as $\alpha \to 0$. Indeed it can be easily shown from Eq. (1.2) that $x_0 \sim (c/\alpha + \zeta_r(\alpha)/\kappa_r(\alpha))$ and $\zeta_r(\alpha) = O(\alpha^2)$, hence $\lim_{\alpha\to 0} f_{r,c}(\alpha) = 0$.

We now show the unimodality of the exponential order.

Proposition 2.5. $\ln f_{r,c}(\alpha)$ *is concave over* $]0, \inf(1,c)]$ *and attains a maximum at some value* $\widehat{\alpha}_{r,c} \in]0, \inf(1,c)[$.

Proof. $\ln(f_{r,c}(\alpha)) = -(1-\alpha)\ln(1-\alpha) - \alpha\ln(\alpha) + \alpha\ln(2(e^{x_0} - 1)) + \zeta_r(\alpha)\kappa_r(\alpha)x_0 - c + c\ln(c\kappa_r(\alpha)/x_0\phi_r)$.

Allowing for

$$1 - e^{-x_0} - \frac{\alpha x_0}{c - x_0 \dfrac{\zeta_r(\alpha)}{\kappa_r(\alpha)}} = 0 \tag{2.28}$$

the first derivative is

$$\frac{d\ln f_{r,c}(\alpha)}{d\alpha} = \ln(1-\alpha) - \ln(\alpha) + \ln(2(e^{x_0} - 1)) - (r-1)\frac{\alpha}{2-\alpha}\frac{x_0}{e^{x_0} - 1}$$

and the second derivative is

$$\frac{\mathrm{d}^2 \ln f_{r,c}(\alpha)}{\mathrm{d}\alpha^2} = -\frac{1}{1-\alpha} - \frac{1}{\alpha} + \frac{\mathrm{d}x_0}{\mathrm{d}\alpha}\left(\frac{\mathrm{e}^{x_0}}{\mathrm{e}^{x_0}-1} + (r-1)\frac{\alpha}{2-\alpha}\frac{\mathrm{e}^{x_0}(x_0-1)+1}{(\mathrm{e}^{x_0}-1)^2}\right)$$
$$-(r-1)\frac{2}{(2-\alpha)^2}\frac{x_0}{\mathrm{e}^{x_0}-1}.$$

It can be easily checked that on $]0, \inf(1,c)[$, $\mathrm{d}x_0/\mathrm{d}\alpha$ is negative and then that $\mathrm{d}^2 \ln f_{r,c}(\alpha)/\mathrm{d}\alpha^2$ is negative. Consequently $\ln f_{r,c}(\alpha)$ is concave on $]0, \inf(1,c)[$. By continuity at $\alpha = \inf(1,c)$, $\ln f_{r,c}(\alpha)$ is concave on $]0, \inf(1,c)]$.

Moreover, since

$$\lim_{\alpha \to 0} \frac{\mathrm{d} \ln f_{r,c}(\alpha)}{\mathrm{d}\alpha} = +\infty \quad \text{and} \quad \lim_{\alpha \to \inf(1,c)} \frac{d \ln f_{r,c}(\alpha)}{\mathrm{d}\alpha} = -\infty,$$

there is a unique value $\widehat{\alpha}_{r,c} \in]0, \inf(1,c)[$ such that $\mathrm{d} \ln f_{r,c}(\alpha)/\mathrm{d}\alpha = 0$. $\widehat{\alpha}_{r,c}$ is therefore the maximum point of $\ln f_{r,c}(\alpha)$ and also of $f_{r,c}(\alpha)$ on $]0, \inf(1,c)]$. □

We give the exponential orders of cumulated expectations. Let ρ be a rational such that $0 < \rho < 1$, we denote by $\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \leqslant \rho n}_{r,c,n}|)$ [resp. $\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \geqslant \rho n}_{r,c}|)$] the expected number of PIs with a length $l \leqslant \rho n$ [resp. $l \geqslant \rho n$].

Proposition 2.6. *ρ being a rational such that $0 < \rho \leqslant \widehat{\alpha}_{r,c}$ [resp. $\widehat{\alpha}_{r,c} \leqslant \rho < 1$], we have* $\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \leqslant \rho n}_{r,c,n}|) \asymp [f_{r,c}(\rho)]^n$ [resp. $\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \geqslant \rho n}_{r,c,n}|) \asymp [f_{r,c}(\rho)]^n$].

Proof. We give the calculation only for $\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \leqslant \rho n}_{r,c}|)$, the calculation for $\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \geqslant \rho n}_{r,c}|)$ is similar. We have

$$\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \leqslant \rho n}_{r,c}|) = \mathbf{E}(|\mathscr{P}\mathscr{I}^{0}_{r,c}|) + \sum_{\alpha = \frac{1}{n}, \frac{2}{n}, \ldots, \frac{\rho n}{n}} \mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|).$$

We know that $\mathbf{E}(|\mathscr{P}\mathscr{I}^{0}_{r,c}|) = 0$ (subsection 2.2). By Relation (2.21) which is valid for any positive rational α, we can write

$$\sum_{\alpha = \frac{1}{n}, \frac{2}{n}, \ldots, \frac{\rho n}{n}} \mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|) \leqslant \sum_{\alpha = \frac{1}{n}, \frac{2}{n}, \ldots, \frac{\rho n}{n}} 2cn \left(1 - \frac{r-1}{n}\right)^{-(r-1)cn}$$
$$\times \sqrt{2\pi\alpha n}\mathrm{e}^{1/12\alpha n}(\mathscr{F}^{\alpha}_{r,c}(\beta^*))^n.$$

By definition $\mathscr{F}^{\alpha}_{r,c}(\beta^*) = f_{r,c}(\alpha)$ and by Proposition 2.5 we can write

$$\sum_{\alpha = \frac{1}{n}, \frac{2}{n}, \ldots, \frac{\rho n}{n}} \mathbf{E}(|\mathscr{P}\mathscr{I}^{\alpha n}_{r,c}|) \leqslant 2c\rho n^2 \left(1 - \frac{r-1}{n}\right)^{-(r-1)cn} \sqrt{2\pi\rho n}\mathrm{e}^{1/12\alpha n}(f_{r,c}(\rho))^n.$$

Hence,

$$\lim_{n \to \infty} \sup[\mathbf{E}(|\mathscr{P}\mathscr{I}^{l \leqslant \rho n}_{r,c}|)]^{1/n} \leqslant f_{r,c}(\rho). \tag{2.29}$$

By Relation (2.23) which is valid for any positive rational α, we can write: for any $\eta>0$ and every $n>\sup(N_1(\eta),N_2(\eta))$:

$$\sum_{\alpha=\frac{1}{n},\frac{2}{n},\ldots,\frac{\rho n}{n}} \mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c}^{\alpha n}|)\geqslant \mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c}^{\rho n}|)\geqslant \mu_{r,c}(\alpha,\widetilde{\beta}_n,n)(\mathscr{F}_{r,c}^{\rho}(\beta^*)-\eta)^n.$$

By definition $\mathscr{F}_{r,c}^{\rho}(\beta^*)=f_{r,c}(\rho)$ and, allowing for (2.26), we have for any $\eta>0$:

$$\lim_{n\to\infty}\inf[\mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c}^{l\leqslant\rho n}|)]^{1/n}\geqslant f_{r,c}(\rho)-\eta.$$

Consequently,

$$\lim_{n\to\infty}\inf[\mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c}^{l\leqslant\rho n}|)]^{1/n}\geqslant f_{r,c}(\rho). \tag{2.30}$$

Finally, by (2.29) and (2.30), we have

$$\lim_{n\to\infty}[\mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c}^{l\leqslant\rho n}|)]^{1/n}=f_{r,c}(\rho). \qquad \square$$

Finally, we state three propositions concerning $f_{r,c}(\alpha)$, which will be useful in the next section. The easy proofs are omitted. For α fixed and c varying, let $g_{r,\alpha}(c)=f_{r,c}(\alpha)$, so that

$$\begin{aligned}\ln g_{r,\alpha}(c) &= \ln f_{r,c}(\alpha)\\ &= -(1-\alpha)\ln(1-\alpha)-\alpha\ln(\alpha)+\alpha\ln(2(e^{x_0}-1))+\frac{\zeta_r(\alpha)}{\kappa_r(\alpha)}x_0-c\\ &\quad +c\ln\left(\frac{c\kappa_r(\alpha)}{x_0\phi_r}\right).\end{aligned}$$

$f_{r,c}(\alpha)$ is defined on $]0,\inf(1,c)]$, and hence $g_{r,\alpha}(c)$ on $[\alpha,+\infty[$.

Proposition 2.7. *$g_{r,\alpha}(c)$ increases from $c=\alpha$ to*

$$c=\widehat{c}_{r,\alpha}=\frac{2^r}{r(2-\alpha)^{r-1}}\ln\left(\frac{2+\alpha r-\alpha}{2-\alpha}\right),$$

attains an absolute maximum at $\widehat{c}_{r,\alpha}$ which is such that

$$\ln g_\alpha(\widehat{c}_{r,\alpha})=-(1-\alpha)\ln(1-\alpha)+\alpha\ln\left(\frac{2r}{2-\alpha}\right)-\frac{2+\alpha r-\alpha}{r}\ln\left(\frac{2+\alpha r-\alpha}{2-\alpha}\right)$$

and then decreases and tends to $-\infty$ as $c\to+\infty$.

Let $h_r(\alpha)=g_\alpha(\widehat{c}_{r,\alpha})$ so that

$$\begin{aligned}\ln h_r(\alpha)=\ln g_\alpha(\widehat{c}_{r,\alpha}) &= -(1-\alpha)\ln(1-\alpha)+\alpha\ln\left(\frac{2r}{2-\alpha}\right)-\frac{2+\alpha r-\alpha}{r}\\ &\quad \ln\left(\frac{2+\alpha r-\alpha}{2-\alpha}\right)\end{aligned}$$

$h_r(\alpha)$ is defined on $[0,1]$.

Proposition 2.8. *$h_r(\alpha)$ increases from $h_r(0)=1$, attains a positive absolute maximum and then decreases down to $h_r(1)=g_1(\widehat{c}_{r,1})=2r/(r+1)^{(r+1)/r}$.*

For $\alpha=c\leqslant 1$, let $k_r(c)=f_{r,c}(c)$, so that

$$\ln k_r(c)=-(1-c)\ln(1-c)-c+c\ln(r)+(r-1)c\ln(1-c/2).$$

$k_r(c)$ is defined on $[0,1]$.

Proposition 2.9. *$k_r(c)$ increases from $k_r(0)=1$ to a positive absolute maximum and then decreases down to $r/2^{r-1}\mathrm{e}<1$.*

3. Bounds for the lengths of prime implicants and for the number of solutions of a random r-CNF formula

In this section we prove Theorems 1.3–1.5 on lower and upper bounds of the normalized lengths of PIs, and Theorems 1.6 and 1.7 on the lower bounds of the actual number of solutions. In a first subsection, Theorems 1.3, 1.4 and 1.6 concerning 2- and 3-CNF formulae are proved, then in a second subsection Theorem 1.3 is extended to r-CNF formulae with $r\geqslant 4$ and Theorems 1.5 and 1.7 concerning those formulae are proved.

Recall that the bounds on normalized lengths of PIs are obtained by calculating bounds of the lengths of PIs and by using the bounds on the actual number of variables given by Proposition 1.1. In both subsections, in order to show that the bounds obtained for the normalized lengths of PIs are better than the obvious ones, we will need to compare the magnitude of the coefficient $1-\mathrm{e}^{-rc}$ in the expectation of the actual number of variables of formulae in $\Omega(n,c,r)$ (see Section 1) with the magnitude of the maximum point $\widehat{\alpha}_{r,c}$ of $f_{r,c}(\alpha)$.

Proposition 3.1. *For every $c>0$ we have $1-\mathrm{e}^{-rc}>\widehat{\alpha}_{r,c}$.*

Proof. Recall that $\tilde{c}_r$ is such that $1-\mathrm{e}^{-r\tilde{c}_r}=\tilde{c}_r$ (Section 1). First we observe that since $\widehat{\alpha}_{r,c}\in\,]0,\inf(1,c)[$ then for $c\in\,]0,\tilde{c}_r[$, $0<\widehat{\alpha}_{r,c}<c$ and $\widehat{\alpha}_{r,c}<1-\mathrm{e}^{-rc}$. For $c\in[\tilde{c}_r,+\infty[$, by Proposition 2.5 it is sufficient to show that $(\mathrm{d}\ln f_{r,c}/\mathrm{d}\alpha)(1-\mathrm{e}^{-rc})<0$. We have

$$\frac{\mathrm{d}\ln f_{r,c}}{\mathrm{d}\alpha}(1-\mathrm{e}^{-rc})=-rc-\ln(1-\mathrm{e}^{-rc})+\ln(2(\mathrm{e}^{x_0}-1))-(r-1)\times\frac{1-\mathrm{e}^{-rc}}{1+\mathrm{e}^{-rc}}\frac{x_0}{\mathrm{e}^{x_0}-1}. \tag{3.1}$$

It can be shown that for $\alpha=1-\mathrm{e}^{-rc}$, the root x_0 of Eq. (1.2) is such that $x_0\leqslant(2r/(2^{r+1}-r-2))(c-\tilde{c}_r)$ (for this check that $(2r/(2^{r+1}-r-2))(c-\tilde{c}_r)<c\kappa_r(1-\mathrm{e}^{-rc})/\zeta_r(1-\mathrm{e}^{-rc})$ and then check that the left-hand side of (1.2) is not positive, substituting $(2r/(2^{r+1}-r-2))(c-\tilde{c}_r)$ for x). Substituting the coarse estimate $(2rc/(2^{r+1}-r-2))$

for x_0 in the term $\ln(2(e^{x_0}-1))$ of (3.1) we have

$$\frac{d\ln f_{r,c}}{d\alpha}(1-e^{-rc}) \leqslant -rc\left(1-\frac{2}{2^{r+1}-r-2}\right) - \ln\left(\frac{1-e^{-rc}}{1-e^{-(2rc/(2^{r+1}-r-2))}}\right) + \ln 2 - (r-1)\frac{1-e^{-rc}}{1+e^{-rc}}\frac{x_0}{e^{x_0}-1}.$$

Since $rc \geqslant r\tilde{c}_r \geqslant 3/2$, we easily check that $-rc(1-2/(2^{r+1}-r-2))+\ln 2<0$. Thereby, $(d\ln f_{r,c}/d\alpha)(1-e^{-rc})<0$. □

3.1. Bounds for 2 and 3-CNF formulae

In this subsection r takes only the value 2 or 3. The determination of lower and upper bounds on the lengths of PIs is based on the fact that $\ln f_{r,c}(\alpha)$ is concave on $]0,\inf(1,c)]$ and on the possible existence of two intersection points of $f_{r,c}(\alpha)$ with the line $y=1$, one point being lower than $\widehat{\alpha}_{r,c}$ and denoted by $\alpha'_m(c)$ if it exists, the other one greater than $\widehat{\alpha}_{r,c}$ and denoted by $\alpha'_M(c)$ if it exists. The following proposition establishes under which conditions these points exist.

Proposition 3.2. *Let $c_r^0<1$ be the unique positive root of*

$$\ln k_r(c) = -(1-c)\ln(1-c) - c + c\ln(r) + (r-1)c\ln(1-c/2) = 0.$$

For any positive $c \leqslant c_r^0$ such that $f_{r,c}(\widehat{\alpha}_{r,c}) \geqslant 1$, there exists one and only one point $\alpha'_m(c)$ such that $0<\alpha'_m(c)\leqslant\widehat{\alpha}_{r,c}$ and $f_{r,c}(\alpha'_m(c))=1$. For any $c>c_r^0$, such that $f_{r,c}(\widehat{\alpha}_{r,c}) \geqslant 1$, there exist two points denoted $\alpha'_m(c)$ and $\alpha'_M(c)$ such that $0<\alpha'_m(c)\leqslant\widehat{\alpha}_{r,c}\leqslant\alpha'_M(c) < \inf(1,c)$ and $f_{r,c}(\alpha'_m(c))=f_{r,c}(\alpha'_M(c))=1$.

Proof. For some $c>0$ assume that $f_{r,c}(\widehat{\alpha}_{r,c})\geqslant 1$. As already mentioned in Section 2.3, $\lim_{\alpha\to 0} f_{r,c}(\alpha)=0$. By the intermediate value theorem, there exists a value which we denote by $\alpha'_m(c)$, such that $0<\alpha'_m(c)\leqslant\widehat{\alpha}_{r,c}$ and $f_{r,c}(\alpha'_m(c))=1$.

Assume that $c_r^0<c\leqslant 1$. By Proposition 2.9 we have $k_r(c)=f_{r,c}(c)<1$. By Proposition 2.5 and the intermediate value theorem, there exists a value which we denote by $\alpha'_M(c)$, such that $\widehat{\alpha}_{r,c}\leqslant\alpha'_M(c)<1$ and $f_{r,c}(\alpha'_M(c))=1$.

Now assume that $c>1$. By Proposition 2.8 $\sup_{c\in]1,+\infty[}[f_{r,c}(1)]=g_1(\widehat{c}_{r,1})=2r/(r+1)$ $(r+1)/r<1$ for $r=2,3$. Again for the same reasons there exists a value $\alpha'_M(c)$, such that $\widehat{\alpha}_{r,c}\leqslant\alpha'_M(c)<1$ and $f_{r,c}(\alpha'_M(c))=1$. □

Now we can prove the theorem on the lower bound of normalized lengths of PIs for 2- and 3-CNF formulae.

Proof of Theorem 1.3. Assume first that for some $c>0$, $f_{r,c}(\widehat{\alpha}_{r,c})\geqslant 1$. By Proposition 3.2, there exists a value $\alpha'_m(c)$, such that $0<\alpha'_m(c)\leqslant\widehat{\alpha}_{r,c}$ and $f_{r,c}(\alpha'_m(c))=1$. Moreover, by Proposition 3.1 we have $\alpha'_m(c)<1-e^{-rc}$. Thus $\alpha'_m(c)/(1-e^{-rc})$ is

within the interval $]0,1[$. By Proposition 2.6 for any $\varepsilon_1 > 0$ such that $\varepsilon_1 < \alpha_m^r(c)$:

$$\mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c,n}^{l \leqslant (\alpha_m^r(c)-\varepsilon_1)n}|) \asymp [f_{r,c}(\alpha_m^r(c) - \varepsilon_1)]^n.$$

Since $0 < \alpha_m^r(c) - \varepsilon_1 < \alpha_m^r(c) \leqslant \widehat{\alpha}_{r,c}$, then $0 < f_{r,c}(\alpha_m^r(c) - \varepsilon_1) < f_{r,c}(\alpha_m^r(c)) = 1$. Hence,

$$\lim_{n \to \infty} \mathbf{Pr}(|\mathscr{P}\mathscr{I}_{r,c,n}^{l \leqslant (\alpha_m^r(c)-\varepsilon_1)n}| > 0) = 0.$$

Let Ψ be the number of variables occurring in a random formula of $\Omega(n,c,r)$, by Proposition 1.1, for any $\varepsilon_2 > 0$:

$$\lim_{n \to \infty} \mathbf{Pr}(\Psi > (1 - \mathrm{e}^{-rc} + \varepsilon_2)n) = 0.$$

Recall that $\mathscr{P}\mathscr{I}_{r,c,n}$ denotes the set of all prime implicants of a random formula of $\Omega(n,c,r)$. $|\mathscr{P}\mathscr{I}_{r,c,n}| = 0$ means that the formula is unsatisfiable. From the two preceding limits it follows:

$$\lim_{n \to \infty} \mathbf{Pr}((|\mathscr{P}\mathscr{I}_{r,c,n}^{l > (\alpha_m^r(c)-\varepsilon_1)n}| = |\mathscr{P}\mathscr{I}_{r,c,n}|) \wedge (\Psi \leqslant (1 - \mathrm{e}^{-rc} + \varepsilon_2)n)) = 1.$$

Choosing appropriately ε_1 and ε_2 as functions of ε we get the statement of the theorem. Now assume that for some $c \geqslant 1$, $f_{r,c}(\widehat{\alpha}_{r,c}) < 1$. By Proposition 2.6 we have:

$$\mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c,n}|) = \sum_{p=1}^{p=n} \mathbf{E}(|\mathscr{P}\mathscr{I}_{r,c,n}^{p}|) \asymp [f_{r,c}(\widehat{\alpha}_{r,c})]^n$$

and therefore a.e. formula in $\Omega(n,c,r)$ is unsatisfiable. □

Now we deal with the upper bound. But first we need to establish three additional facts concerning $\alpha_M^r(c)$ for the values of c, where it exists, which will enable us to show that $\alpha_M^r(c)/(1 - \mathrm{e}^{-rc})$ is lower than 1.

Proposition 3.3. *For any $c \in [c_r^0, +\infty[$ such that $\alpha_M^r(c)$ exists we have $\alpha_M^r(c) \leqslant \mathring{\alpha}_r = \alpha_M^r(\widehat{c}_{r,\mathring{\alpha}_r})$ where $\mathring{\alpha}_r$ is the unique positive root of*

$$\ln h_r(\alpha) = -(1-\alpha)\ln(1-\alpha) + \alpha \ln\left(\frac{2r}{2-\alpha}\right) - \frac{2 + \alpha r - \alpha}{r} \ln\left(\frac{2 + \alpha r - \alpha}{2 - \alpha}\right) = 0.$$

Proof. By Proposition 2.8, for $r = 2, 3$, $h_r(1) = 2r/(r+1)^{(r+1)/r} < 1$ and therefore $\ln h_r(\alpha)$ has a unique positive root which we denote by $\mathring{\alpha}_r$. By Propositions 2.7 and 2.8 for every $\alpha > \mathring{\alpha}_r$ there is no $c \geqslant \alpha$ such that $g_{r,\alpha}(c) = f_{r,c}(\alpha) = 1$. Hence for every $c \in [c_r^0, +\infty[$ such that $\alpha_M^r(c)$ exists so that $f_{r,c}(\alpha_M^r(c)) = 1$, we have $\alpha_M^r(c) \leqslant \mathring{\alpha}_r$.

Recall (Proposition 2.7) that

$$\widehat{c}_{r,\alpha} = \frac{2^r}{r(2-\alpha)^{r-1}} \ln\left(\frac{2 + \alpha r - \alpha}{2 - \alpha}\right).$$

We have $h_r(\mathring{\alpha}_r) = g_{r,\mathring{\alpha}_r}(\widehat{c}_{r,\mathring{\alpha}_r}) = f_{r,\widehat{c}_{r,\mathring{\alpha}_r}}(\mathring{\alpha}_r) = 1$. Moreover

$$\frac{\mathrm{d} \ln f_{r,\widehat{c}_{r,\alpha}}(\alpha)}{\mathrm{d}\alpha} = \frac{d \ln g_{r,\alpha}(\widehat{c}_{r,\alpha})}{\mathrm{d}\alpha} = \frac{d \ln h_r(\alpha)}{\mathrm{d}\alpha}.$$

From the variations of $\ln h_r(\alpha)$ (Proposition 2.8) we have $(\mathrm{d}\ln h/\mathrm{d}\alpha)(\mathring{\alpha}_r)<0$. $f_{r,\widehat{c}_{r,\mathring{\alpha}_r}}(\mathring{\alpha}_r)=1$ and $(\mathrm{d}\ln h/\mathrm{d}\alpha)(\mathring{\alpha}_r)=(\mathrm{d}\ln f_{r,\widehat{c}_{r,\alpha}}/\mathrm{d}\alpha)(\mathring{\alpha}_r)<0$ implies $\mathring{\alpha}_r=\alpha_M^r(\widehat{c}_{r,\mathring{\alpha}_r})$. □

Proposition 3.4. *The equation $f_{r,c}(\alpha)=1$ defines $\alpha_M^r(c)$ as a continuous increasing implicit function on $[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}[$.*

Proof. First we prove that $\alpha_M^r(c)$ is defined on $[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}[$. By Proposition 2.8, for every $\alpha\in[0,\mathring{\alpha}_r[$, $h_r(\alpha)=\ln g_{r,\alpha}(\widehat{c}_{r,\alpha})>0$.

$$\widehat{c}_{r,\alpha}=\frac{2^r}{r(2-\alpha)^{r-1}}\ln\left(\frac{2+\alpha r-\alpha}{2-\alpha}\right)$$

being strictly increasing in α on $[0,1]$, for every $c\in[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}[$ there is one value, which we denote by $\alpha_{r,c}$, such that $\alpha_{r,c}\in[0,\mathring{\alpha}_r[$ and $\widehat{c}_{r,\alpha_{r,c}}=c$ and $g_{r,\alpha_c}(\widehat{c}_{r,\alpha_{r,c}})=f_{r,c}(\alpha_{r,c})>1$. Thereby we have $f_{r,c}(\widehat{\alpha}_{r,c})>1$ and by Proposition 3.2 $\alpha_M^r(c)$ is well-defined on $[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}[$. And since $\alpha_M^r(\widehat{c}_{r,\mathring{\alpha}_r})=\mathring{\alpha}_r$, $\alpha_M^r(c)$ is also defined at $\widehat{c}_{r,\mathring{\alpha}_r}$. Therefore $\alpha_M^r(c)$ is an implicit function of c on $[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}]$.

From the above we can deduce that for every $c\in[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}[$ we have $\alpha_M^r(c)>\widehat{\alpha}_{r,c}$ and therefore $(\mathrm{d}\ln f_{r,c}/\mathrm{d}\alpha)(\alpha_M^r(c))<0$. At $c=\widehat{c}_{r,\mathring{\alpha}_r}$ we have also $(\mathrm{d}\ln f_{r,c}/\mathrm{d}\alpha)(\alpha_M^r(\widehat{c}_{r,\mathring{\alpha}_r}))<0$ (see proof of Proposition 3.3). It follows that $\alpha_M^r(c)$ is a continuous implicit function on $[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}]$.

Finally, we prove that $\alpha_M^r(c)$ is increasing on $[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}]$. It can be observed that $g_{r,\alpha}(\alpha)=k_r(\alpha)$ (Proposition 2.9). Let $\alpha_0^r=c_r^0$. It can be easily shown that $\alpha_0^r<\mathring{\alpha}_r$. By Proposition 2.9, we have $g_{r,\alpha_0^r}(\alpha_0^r)=k_r(c_r^0)=1$, for every $\alpha\in]0,\alpha_0^r[$, $g_{r,\alpha}(\alpha)>1$ and for every $\alpha\in]\alpha_0^r,\mathring{\alpha}_r[$, $g_{r,\alpha}(\alpha)<1$. From this and from Propositions 2.7 and 2.8, it can be deduced that for every $\alpha\in]0,\alpha_0^r[$ there is exactly one value of c, say c', such that $g_{r,\alpha}(c')=f_{r,c'}(\alpha)=1$ and for every $\alpha\in]\alpha_0^r,\mathring{\alpha}_r[$ there are exactly two values of c, say c' and c'', such that $g_{r,\alpha}(c')=f_{r,c'}(\alpha)=g_{r,\alpha}(c'')=f_{r,c''}(\alpha)=1$. It is then an easy exercise, using the intermediate value theorem, to show that for any pair $c',c''\in[c_r^0,\widehat{c}_{r,\mathring{\alpha}_r}]$, we have $c'<c''\Rightarrow\alpha_M^r(c')<\alpha_M^r(c'')$. □

Proposition 3.5. *For $r=2,3$ and for any $c\geqslant c_r^0$ such that $\alpha_M^r(c)$ exists, we have $\alpha_M^r(c)<1-\mathrm{e}^{-rc}-\tau_r$ with $\tau_2=0.03$ and $\tau_3=0.012$.*

Proof. Let us take first $r=3$. Let $\phi_{r,c}(x_0,\alpha)=f_{r,c}(\alpha)$ and let $\phi_{r,c}(x,\alpha)$ be the extension of $\phi_{r,c}(x_0,\alpha)$ to $[0,\infty[\times]0,1]$. For α fixed, $\phi_{r,c}(x,\alpha)$ is minimum at $x=x_0$. Let $\psi_{r,c}(x_0,\alpha)=(\mathrm{d}f_{r,c}/\mathrm{d}\alpha)(\alpha)$ and let $\psi_{r,c}(x,\alpha)$ be the extension of $\psi_{r,c}(x_0,\alpha)$ to $]0,\infty[\times]0,1[$. For α fixed, $\psi_{r,c}(x,\alpha)$ increases with x. Let us define the three following sequences of numbers: $(\lambda_0=0.44,\ \lambda_1=0.785,\ \lambda_2=1.48,\ \lambda_3=2.62)$, $(\delta_1=0.711,\ \delta_2=0.892,\ \delta_3=0.975)$, and $(\mu_1=0.090,\ \mu_2=0.424,\ \mu_3=0.924)$. In the following we use an index i which can take the values 1, 2 or 3. It can be easily checked by Proposition 3.3 that $\mathring{\alpha}_3<0.9875$ and $\widehat{c}_{3,\mathring{\alpha}_3}<3.556$. Thereby by Proposition 3.4 we deduce that $\alpha_M^3(\lambda_i)$

exists. Moreover, it can be checked that $\phi_{3,\lambda_i}(\mu_i,\delta_i)<0$, which implies $f_{3,\lambda_i}(\delta_i)<0$. For $c=\lambda_i$ and $x=\mu_i$ it can be checked that the left hand-side of Eq. (1.2) is negative which implies that the root $x_0(\lambda_i)$ of (1.2) is strictly smaller than μ_i. And since it can be also checked that $\psi_{3,\lambda_i}(\mu_i,\delta_i)<0$, we have $(\mathrm{d}f_{3,\lambda_i}/\mathrm{d}\alpha)(\delta_i)<0$. From $f_{3,\lambda_i}(\delta_i)<0$ and $(\mathrm{d}f_{3,\lambda_i}/\mathrm{d}\alpha)(\delta_i)<0$ we deduce $\alpha^3_M(\lambda_i)<\delta_i$ and since $\delta_i<1-\mathrm{e}^{-3\lambda_{i-1}}-\tau_3$ then $\alpha^3_M(\lambda_i)<1-\mathrm{e}^{-3\lambda_{i-1}}-\tau_3$. Finally, it can be checked that $\lambda_0<c^0_3$ and $\mathring{\alpha}_3<0.9875<1-\mathrm{e}^{-3\lambda_3}-\tau_3$. $\alpha^3_M(c)$ being continuous and increasing on $[c^0_3,\widehat{c}_{r,\alpha_3}{}^{\circ}]$ (Proposition 3.4), from $\alpha^3_M(\lambda_i)<1-\mathrm{e}^{-3\lambda_{i-1}}-\tau_3$ with $i=1,2,3$, it follows that for every $c\in[c^0_3,\widehat{c}_{3,\alpha_3}{}^{\circ}]$ we have $\alpha^3_M(c)<1-\mathrm{e}^{-3c}-\tau_3$. $\mathring{\alpha}_3$ being, by Proposition 3.3, the maximum of all $\alpha^3_M(c)$ (i.e. for all c in $[c^0_3,\infty[$ where $\alpha^3_M(c)$ exists), and since $\mathring{\alpha}_3<1-\mathrm{e}^{-3\widehat{c}_{3,\alpha_3}{}^{\circ}}-\tau_3$, then for any $c\in[\widehat{c}_{3,\alpha_3}{}^{\circ},\infty[$ such that $\alpha^3_M(c)$ exists, we obviously have $\alpha^3_M(c)<1-\mathrm{e}^{-3c}-\tau_3$. To sum up, for any $c\in[c^0_3,\infty[$ such that $\alpha^3_M(c)$ exists we have $\alpha^3_M(c)<1-\mathrm{e}^{-3c}-\tau_3$.

For $r=2$, taking the three sequences of numbers ($\lambda_0=0.52$, $\lambda_1=0.621$, $\lambda_2=0.727$, $\lambda_3=0.836$, $\lambda_4=0.956$, $\lambda_5=1.095$, $\lambda_6=1.276$), ($\delta_1=0.611$, $\delta_2=0.680$, $\delta_3=0.735$, $\delta_4=0.781$, $\delta_5=0.821$, $\delta_6=0.857$), and ($\mu_1=0.025$, $\mu_2=0.093$, $\mu_3=0.173$, $\mu_4=0.267$, $\mu_5=0.381$, $\mu_5=0.534$), in a similar way to $r=3$ above, it can be proved that for any $c\in[c^0_2,\infty[$ such that $\alpha^2_M(c)$ exists we have: $\alpha^2_M(c)<1-\mathrm{e}^{-2c}-\tau_2$. □

We can now prove Theorems 1.4 and 1.6.

Proof of Theorem 1.4. Assume first that for some $c\geqslant c^0_r$, $f_{r,c}(\widehat{\alpha}_{r,c})\geqslant 1$. By Proposition 3.2, there exists a value $\alpha^r_M(c)$ such that $\widehat{\alpha}_{r,c}\leqslant\alpha^r_M(c)<1$ and $f_{r,c}(\alpha^r_M(c))=1$. From Proposition 3.5 it can be deduced directly that $\alpha^r_M(c)/(1-\mathrm{e}^{-rc})$ is within the interval $]0,1[$. The proof of the core of the statement of the theorem is similar to that for the lower bound (Theorem 1.3), but the direction of inequalities must be inverted. □

From that, Theorem 1.6 is proved easily.

Proof of Theorem 1.6. The bound $2^{(1-\mathrm{e}^{-rc}-\alpha^r_M(c)-\varepsilon)n}$ as a function of c is directly derived from Theorem 1.4. Allowing for the inequality of Proposition 3.5, we can directly set the absolute lower bounds $2^{0.03n}$ for $r=2$ and $2^{0.012n}$ for $r=3$. □

3.1.1. Numerical computations

Tables 1 and 2 list for $r=2$ and $r=3$ respectively, values of $\alpha^r_m(c)/(1-\mathrm{e}^{-rc})$, $\alpha^r_M(c)/(1-\mathrm{e}^{-rc})$ and of the exponent $1-\mathrm{e}^{-rc}-\alpha^r_M(c)$ of the lower bound $2^{(1-\mathrm{e}^{-rc}-\alpha^r_M(c)-\varepsilon)n}$ of numbers of solutions (Theorem 1.6). These values were computed for values of the ratio c, from c^0_r up to values which are for $r=2$ at most equal to the value of the threshold $c=1$ and for $r=3$, close to the expected value of the threshold from experiments. Of course the listed values make sense only if for the chosen values of c, not a.e. formula in $\Omega(n,c,r)$ is unsatisfiable. We computed the values of $\alpha^r_m(c)$ and $\alpha^r_M(c)$ by solving equation $\ln f_{r,c}(\alpha)=0$. $\ln f_{r,c}(\alpha)$ is concave and increasing

Table 1

2-CNF formulae $c=\frac{\#\text{clauses}}{\#\text{variables}}$	Normalized length of PIs (lower bound) $\frac{\alpha_m^r(c)}{1-e^{-rc}}$	(upper bound) $\frac{\alpha_M^r(c)}{1-e^{-rc}}$	#solutions (lower bound) $2^{(1-e^{-rc}-\alpha_M^r(c))n}$
0.6	0.437	0.851	$2^{0.104n}$
0.7	0.457	0.881	$2^{0.090n}$
0.8	0.477	0.899	$2^{0.080n}$
0.9	0.499	0.912	$2^{0.074n}$
1.0	0.521	0.919	$2^{0.069n}$

Table 2

3-CNF formulae $c=\frac{\#\text{clauses}}{\#\text{variables}}$	Normalized length of PIs (lower bound) $\frac{\alpha_m^r(c)}{1-e^{-rc}}$	(upper bound) $\frac{\alpha_M^r(c)}{1-e^{-rc}}$	#solutions (lower bound) $2^{(1-e^{-rc}-\alpha_M^r(c))n}$
0.6	0.287	0.718	$2^{0.116n}$
1	0.360	0.833	$2^{0.117n}$
1.5	0.448	0.905	$2^{0.083n}$
2	0.528	0.947	$2^{0.050n}$
2.5	0.600	0.971	$2^{0.028n}$
3	0.665	0.984	$2^{0.016n}$
3.5	0.726	0.988	$2^{0.012n}$
4	0.784	0.985	$2^{0.015n}$
4.25	0.814	0.981	$2^{0.019n}$
4.5	0.846	0.974	$2^{0.026n}$

(resp. decreasing) on $]0,\widehat{\alpha}_{r,c}[$ (resp. on $]\widehat{\alpha}_{r,c},1]$). Consequently Newton's method can be used to compute the lower root $\alpha_m^r(c)$ (resp. upper root $\alpha_M^r(c)$) of $\ln f_{r,c}(\alpha)=0$. For the computation, the starting points $\alpha_s(c)$ must be chosen, positive and sufficiently low (resp. high) so that $f_{r,c}(\alpha_s(c))<0$. Values x_0 necessary to evaluate $\ln f_{r,c}(\alpha)$ were computed by solving equation (1.2) in the following way. Putting $u(x)=1-e^{-x}$ and $v(x)=\alpha x/(c-x\,\zeta_r(\alpha)/\kappa_r(\alpha))$, it can be noted that on the one hand $u(x)$ is positive and concave, and on the other hand for $x<c\,\kappa_r(\alpha)/(\zeta_r(\alpha))$, $v(x)$ is positive and convex. Moreover we have $u'(x)<\infty$ and $v'(x)<\infty$. And $v(x)$ being explicitly invertible then $v^{-1}(x)$ can then be numerically computed. Consequently a simple iteration method can be applied to solve $u(x)=v(x)$ and to find the root x_0. For the computation, a starting point x_s must be chosen positive and such that $u(x_s)>v(x_s)$.

3.2. Bounds for r-CNF formulae with $r\geqslant 4$

We first extend to r-CNF formulae with $r\geqslant 4$, Theorem 1.3 on the lower bound of PIs proved for 2- and 3-CNF formulae in the preceding subsection. The conditions of existence of a lower intersection point of $f_{r,c}(\alpha)$ with the line $y=1$ for 2- and 3-CNF formulae stated in Proposition 3.2 obviously hold for r-CNF formulae with $r\geqslant 4$. Thus:

Proposition 3.6. *For every $c>0$ such that $f_{r,c}(\alpha)\geqslant 1$ there exists a point denoted by $\alpha_m^r(c)$ such that $0<\alpha_m^r(c)\leqslant\widehat{\alpha}_{r,c}$ and $f_{r,c}(\alpha_m^r(c))=1$.*

It follows that the proof of Theorem 1.3 for 2- and 3-CNF formulae holds for r-CNF formulae with $r\geqslant 4$.

To prove Theorems 1.5 and 1.7, we determine as for Theorems 1.4 and 1.6, the conditions of existence of an upper intersection point $\alpha_M^r(c)$ of $f_{r,c}(\alpha)$ with $y=1$ such that $\alpha_M^r(c)<1-\mathrm{e}^{-rc}$. For $r\geqslant 4$, this can be done by studying directly the variations of $f_{r,c}(1-\mathrm{e}^{-rc})$. That did not seem easy for $r=2,3$, the reason why a specific calculation was made in the preceding subsection to prove that when $\alpha_M^r(c)$ exists, we have $\alpha_M^r(c)<1-\mathrm{e}^{-rc}$. We first prove:

Proposition 3.7. $\ln f_{r,c}(1-\mathrm{e}^{-rc})$ *is concave on* $]\tilde{c}_r,+\infty[$.

Proof. We prove that for any $c\in]\tilde{c}_r,+\infty[$ we have $(\mathrm{d}^2/\mathrm{d}c^2)\ln f_{r,c}(1-\mathrm{e}^{-rc})\leqslant 0$. Let $\gamma=1-\mathrm{e}^{-rc}$. We have

$$\frac{\mathrm{d}^2}{\mathrm{d}c^2}\ln f_{r,c}(1-\mathrm{e}^{-rc})=\frac{\mathrm{d}}{\mathrm{d}c}\left(\frac{\mathrm{d}}{\mathrm{d}\gamma}\ln f_{r,c}(\gamma)\frac{\mathrm{d}\gamma}{\mathrm{d}c}\right)+\frac{\mathrm{d}^2}{\mathrm{d}c^2}\ln(f_{r,c}(\gamma)).$$

Hence,

$$\begin{aligned}
&\frac{\mathrm{d}^2}{\mathrm{d}c^2}\ln f_{r,c}(1-\mathrm{e}^{-rc})\\
&\quad=\left(-\frac{1}{1-\gamma}-\frac{1}{\gamma}-(r-1)\frac{2}{(2-\gamma)^2}\frac{x_0}{\mathrm{e}^{x_0}-1}\right)\left(\frac{\mathrm{d}\gamma}{\mathrm{d}c}\right)^2\\
&\qquad+\left(\frac{\mathrm{e}^{x_0}}{\mathrm{e}^{x_0}-1}+(r-1)\frac{\gamma}{2-\gamma}\frac{\mathrm{e}^{x_0}(x_0-1)+1}{(\mathrm{e}^{x_0}-1)^2}\right)\frac{\mathrm{d}x_0}{\mathrm{d}c}\frac{\mathrm{d}\gamma}{\mathrm{d}c}\\
&\qquad+\left(\ln(1-\gamma)-\ln(\gamma)+\ln(2(\mathrm{e}^{x_0}-1))-(r-1)\frac{\gamma}{2-\gamma}\frac{x_0}{\mathrm{e}^{x_0}-1}\right)\frac{\mathrm{d}^2\gamma}{\mathrm{d}c^2}\\
&\qquad+\frac{1}{c}-\frac{(r-1)}{2-\gamma}r\mathrm{e}^{-rc}-\frac{1}{x_0}\frac{\mathrm{d}x_0}{\mathrm{d}c}.
\end{aligned}\tag{3.2}$$

Considering that

$$\frac{\mathrm{d}x_0}{\mathrm{d}c}=\frac{1-\left(\frac{\mathrm{d}}{\mathrm{d}\gamma}\left(\frac{\zeta_r(\gamma)}{\kappa_r(\gamma)}\right)+\frac{1}{1-\mathrm{e}^{-x_0}}\right)x_0\frac{\mathrm{d}\gamma}{\mathrm{d}c}}{\frac{\zeta_r(\gamma)}{\kappa_r(\gamma)}+\frac{\gamma}{1-\mathrm{e}^{-x_0}}-\frac{\gamma x_0\mathrm{e}^{-x_0}}{(1-\mathrm{e}^{-x_0})^2}}$$

and bounding terms on the right-hand side of (3.2) yields

$$\begin{aligned}
\frac{\mathrm{d}^2}{\mathrm{d}c^2}\ln f_{r,c}(1-\mathrm{e}^{-rc})\leqslant&\left[\left(-2^{r+1}+r2^r+rc2^r+\frac{(r-1)}{2}+\frac{(r-1)}{r}(2^r-1)\right)\right.\\
&\left.\times\frac{x_0}{1+x_0}+\frac{2^r}{\mathrm{e}}+2-\frac{\mathrm{e}^{rc}-1}{rc}\mathrm{e}^{-x_0}\right]\frac{1+x_0}{x_0}r\mathrm{e}^{-rc}.
\end{aligned}$$

As already mentioned in the proof of Proposition 3.1, we have $x_0 \leqslant (2r/(2^{r+1}-r-2))(c-\tilde{c}_r)$. Allowing for $x_0/(1+x_0) \leqslant x_0$, we have

$$\frac{d^2}{dc^2} \ln f_{r,c}(1-e^{-rc}) \leqslant \left[\left(-2^{r+1}+r2^r+rc2^r+\frac{(r-1)}{2}+\frac{(r-1)}{r}(2^r-1)\right) \times \frac{2r}{2^{r+1}-r-2}(c-\tilde{c}_r)+\frac{2^r}{e}+2-\frac{e^{rc}-1}{rc}e^{-(2r/(2^{r+1}-r-2))} \times (c-\tilde{c}_r)\right]\frac{1+x_0}{x_0}re^{-rc}.$$

Let:

$$\delta_r(c)=\left(-2^{r+1}+r2^r+rc2^r+\frac{(r-1)}{2}+\frac{(r-1)}{r}(2^r-1)\right)\frac{2r}{2^{r+1}-r-2}(c-\tilde{c}_r) +\frac{2^r}{e}+2-\frac{e^{rc}-1}{rc}e^{-(2r/(2^{r+1}-r-2))}(c-\tilde{c}_r).$$

To prove $(d^2/dc^2)\ln f_{r,c}(1-e^{-rc}) \leqslant 0$, it is sufficient to prove $\delta_r(c) \leqslant 0$. We will deal with the case $r=4$ in a specific way after the general case $r \geqslant 5$. Using the following inequalities:

$$-2^{r+1}+\frac{(r-1)}{2}+\frac{(r-1)}{r}(2^r-1)<0 \quad \text{and} \quad e^{rc}-1 \geqslant \frac{rce^{rc}}{1+rc},$$

we can write

$$\delta_r(c) \leqslant \frac{1}{1+rc}\left(2^r r(c+1)\frac{2r}{2^{r+1}-r-2}(c-\tilde{c}_r)(1+rc) +\left(\frac{2^r}{e}+2\right)(1+rc)-e^{rc-(2r/(2^{r+1}-r-2))}(c-\tilde{c}_r)\right).$$

For $r \geqslant 5$, it can be shown by successive derivations that the second factor on the right-hand side of the above inequality is decreasing on $[\tilde{c}_r, +\infty[$ and is negative for $c=\tilde{c}_r$.

Unfortunately, in the case $r=4$, the above second factor is not decreasing in c. For this special case, we use a more accurate lower bound for $e^{rc}-1$ than the previous one, namely:

$$e^{rc}-1 \geqslant e^{rc}\frac{rc+(rc)^2/2}{1+rc+(rc)^2/2}.$$

Thus,

$$\delta_4(c) \leqslant \frac{1}{1+4c+8c^2}\left[\left(\left(\frac{179}{4}+64c\right)\frac{4}{13}(c-\tilde{c}_4)+\frac{16}{e}+2\right)(1+4c+8c^2) -(1+2c)e^{4c-(4/13)(c-\tilde{c}_4)}\right].$$

As in the general case, it can be shown by successive derivations that the second factor on the right-hand side of the above inequality is decreasing on $[\tilde{c}_4, +\infty[$ and is negative for $c = \tilde{c}_4$. □

We can now give the conditions of existence of an upper intersection point $\alpha_M^r(c)$ of $f_{r,c}(\alpha)$ with $y = 1$ such that $\alpha_M^r(c) < 1 - e^{-rc}$.

Proposition 3.8. *Let $c_r^0 < 1$ be the unique positive root of*

$$\ln k_r(c) = -(1-c)\ln(1-c) - c + c\ln(r) + (r-1)c\ln(1-c/2) = 0$$

and let c_r^1 and c_r^2 be the respective lower and upper roots of $f_{r,c}(1 - e^{-rc}) = 1$. For every $r \geqslant 4$ and for every $c \in]c_r^0, c_r^1[\cup]c_r^2, \infty[$ such that $f_{r,c}(\widehat{\alpha}_{r,c}) \geqslant 1$, there exists a point denoted by $\alpha_M^r(c)$ such that $\widehat{\alpha}_{r,c} \leqslant \alpha_M^r(c) < \inf(1 - e^{-rc}, c)$ and $f_{r,c}(\alpha_M^r(c)) = 1$.

Proof. For every $c \in]c_r^0, \tilde{c}_r[$ by Proposition 2.9 we have $\ln k_r(c) = \ln f_{r,c}(c) < 0$. If $\ln f_{r,c}(\widehat{\alpha}_{r,c}) \geqslant 0$ then by Proposition 2.5 there exists a point $\alpha_M^r(c)$, such that $\widehat{\alpha}_{r,c} \leqslant \alpha_M^r(c) < c$ and $\ln f_{r,c}(\alpha_M^r(c)) = 0$. We show now that the curve $\ln f_{r,c}(1 - e^{-rc})$ intersects the c-axis at two points c_r^1 and c_r^2 such that $\tilde{c}_r < c_r^1 < \widehat{c}_{r,1} < c_r^2$. We prove first that for some $c > \tilde{c}_r$ we have $\ln f_{r,c}(1 - e^{-rc}) > 0$. By Proposition 2.7 at $c = \widehat{c}_{r,1} = (2^r/r)\ln(r+1)$ we have $\ln f_{r,\widehat{c}_{r,1}}(1) = \ln(2r) - ((r-1)/r)\ln(r+1) > 0$. It can be easily shown that $\widehat{c}_{r,1} > \tilde{c}_r$. Moreover, by Proposition 3.1 we have $\ln f_{r,\widehat{c}_{r,1}}(1 - e^{-r\widehat{c}_{r,1}}) \geqslant \ln f_{r,\widehat{c}_{r,1}}(1) > 0$. We can now prove that there exist two intersection points. On the one hand, for $c = \tilde{c}_r$ and $\alpha = 1 - e^{-r\tilde{c}_r} = \tilde{c}_r$ the root x_0 of Eq. (1.2) is 0. We have therefore

$$\ln f_{r,\tilde{c}_r}(1 - e^{-r\tilde{c}_r}) = r\tilde{c}_r e^{-r\tilde{c}_r} - \tilde{c}_r + \tilde{c}_r \ln(r(1 - \tilde{c}_r/2)^{r-1}) < 0.$$

Since $\ln f_{r,\tilde{c}_r}(1 - e^{-r\tilde{c}_r}) < 0$ and $\ln f_{r,\widehat{c}_{r,1}}(1 - e^{-r\widehat{c}_{r,1}}) > 0$, by the intermediate value theorem there exists a point c_r^1 such that $\tilde{c}_r < c_r^1 < \widehat{c}_{r,1}$ and $\ln f_{r,c_r^1}(1 - e^{-rc_r^1}) = 0$. And, by Proposition 3.7, for any $c \in [\tilde{c}_r, c_r^1[$, we have $\ln f_{r,c}(1 - e^{-rc}) < 0$. On the other hand as $c \to +\infty$ we have $x_0 \sim c/(1 + \zeta_r(1)/\kappa_r(1))$ and

$$\ln(f_{r,c}(1 - e^{-rc})) \sim \ln 2 + c\ln\left(\frac{\kappa_r(1)}{\left(1 + \frac{\zeta_r(1)}{\kappa_r(1)}\right)\phi_r}\right)$$

$$= \ln 2 + c\ln\left(\frac{r^2}{(2^r - 1)2^r}\right) \to -\infty.$$

Again by the intermediate value theorem, there exists a point c_r^2 such that $\widehat{c}_{r,1} < c_r^2$ and $\ln f_{r,c_r^2}(1 - e^{-rc_r^2}) = 0$. And, by Proposition 3.7, for any $c \in]c_r^2, +\infty[$, we have $\ln f_{r,c}(1 - e^{-rc}) < 0$. Since we have just proved that for every $c \in [\tilde{c}_r, c_r^1[\cup]c_r^2, \infty[$, $\ln f_{r,c}(1 - e^{-rc}) < 0$, if in addition $\ln f_{r,c}(\widehat{\alpha}_{r,c}) \geqslant 0$, then by Proposition 3.1 there exists

Table 3

4-CNF formulae $c = \frac{\#\text{clauses}}{\#\text{variables}}$	Normalized length of PIs (lower bound) $\frac{\alpha_m^r(c)}{1-e^{-rc}}$
0.6	0.224
1	0.290
2	0.428
3	0.528
4	0.607
5	0.672
6	0.728
7	0.778
8	0.825
9	0.870
9.8	0.910
10	0.922

Table 4

4-CNF formulae $c = \frac{\#\text{clauses}}{\#\text{variables}}$	Normalized length of PIs (upper bound) $\frac{\alpha_M^r(c)}{1-e^{-rc}}$	#solutions (lower bound) $2^{(1-e^{-rc}-\alpha_M^r(c))n}$
$c_4^0 \simeq 0.576 < c < c_4^1 \simeq 4.358$		
0.6	0.653	$2^{0.256n}$
1	0.775	$2^{0.206n}$
2	0.912	$2^{0.087n}$
3	0.970	$2^{0.020n}$
4	0.996	$2^{0.004n}$
$c > c_4^2 \simeq 9.365$		
9.5	0.9991	$2^{0.0009n}$
9.8	0.996	$2^{0.004n}$
10	0.992	$2^{0.008n}$

a point $\alpha_M^r(c)$ such that $\widehat{\alpha}_{r,c} \leqslant \alpha_M^r(c) < 1 - e^{-rc} \leqslant c$ and $\ln f_{r,c}(\alpha_M^r(c)) = 0$. Thus, the proposition is completely proved. □

Using the two preceding propositions, Theorems 1.5 and 1.7 are proved in a similar way to Theorems 1.4 and 1.6.

3.2.1. Numerical computations

Tables 3, 4 and Tables 5, 6 list, for $r=4$ and $r=5$, respectively, and for some values of the ratio c in the intervals $[c_r^0, c_r^1[\cup]c_r^2, \infty[$, values of $\alpha_m^r(c)/(1-e^{-rc})$, $\alpha_M^r(c)/(1-e^{-rc})$ and of the exponent $1-e^{-rc}-\alpha_M^r(c)$ of the lower bound $2^{(1-e^{-rc}-\alpha_M^r(c)-\varepsilon)n}$ of numbers of solutions (Theorem 1.7). As previously for Tables 1 and 2, values listed in Tables 3–6 make sense only if for the chosen values of c, not a.e. formula in $\Omega(n,c,r)$ is unsatisfiable. $\ln f_{r,c}(1-e^{-rc})$ being concave, the roots c_r^1 and c_r^2 were computed by

Table 5

5-CNF formulae $c = \frac{\#\text{clauses}}{\#\text{variables}}$	Normalized length of PIs (lower bound) $\frac{\alpha_m^r(c)}{1-e^{-rc}}$
0.6	0.190
2	0.367
4	0.511
6	0.605
8	0.675
10	0.732
12	0.779
14	0.822
16	0.860
18	0.897
20	0.935
20.8	0.953
21	0.958
21.3	0.968

Table 6

5-CNF formulae $c = \frac{\#\text{clauses}}{\#\text{variables}}$	Normalized length of PIs (upper bound) $\frac{\alpha_M^r(c)}{1-e^{-rc}}$	#solutions (lower bound) $2^{(1-e^{-rc}-\alpha_M^r(c))n}$
$c_5^0 \simeq 0.576 < c < c_5^1 \simeq 6.097$		
0.6	0.611	$2^{0.339n}$
1	0.730	$2^{0.263n}$
2	0.865	$2^{0.135n}$
3	0.927	$2^{0.073n}$
4	0.963	$2^{0.037n}$
5	0.986	$2^{0.014n}$
6	0.9993	$2^{0.0007n}$
$c > c_5^2 \simeq 20.678$		
20.8	0.9994	$2^{0.0006n}$
21	0.998	$2^{0.002n}$
21.3	0.993	$2^{0.007n}$

Newton's method. $\alpha_m^r(c)$ and $\alpha_M^r(c)$ were computed in the same way as for 2- and 3-CNF formulae.

Acknowledgements

We thank P. Flajolet and M. Soria for information on Stirling numbers. We also thank J. Mandler and M. Talagrand for fruitful discussions which improved and clarified the results presented in this paper.

References

[1] V. Chvátal, B. Reed, Miks gets some (the odds are on his side), in: Proc. 33rd IEEE Symp. on Foundations of Computer Science, 1992, pp. 620–627.
[2] J.M. Crawford, L.D. Auton, Experimental results on the crossover point in Satisfiablity Problems, in: Proc. 11th National Conf. on Artificial Intelligence, Washington, D.C., AAAI, New York, 1993, pp. 21–27.
[3] M. Davis, H. Putnam, A computing procedure for quantification theory, J. Assoc. Comput. Mach. 7 (1960) 201–215.
[4] J. de Kleer, An Assumption-Based TMS, Artif. Intell. 28 (1986) 127–162.
[5] O. Dubois, P. André, Y. Boufkhad, J. Carlier, SAT versus UNSAT, in: D.S. Jonhson, M.A. Trick, (Eds.), Second DIMACS Implementation Challenge, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, Providence, RI, 1993.
[6] O. Dubois, Y. Boufkhad, A general upper bound for the satisfiability threshold of random r-sat formulae, J. Algorithms 24 (1997) 395–420.
[7] E. Friedgut, Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-sat problem, submitted.
[8] A. Goerdt, A threshold for unsatisfiability, in: I.M. Havel, V. Koubek (Eds.), Mathematical Foundations of Computer Science, Prague, Czechoslovakia, August 1992, pp. 264–274.
[9] D.F. Hasl, Advanced concepts in fault tree analysis, in: Proc. System Safety Symp. Seatle, June, 1965.
[10] N.L. Johnson, S. Kotz, Urn Models and their Applications, Wiley, New York, 1977.
[11] V.F. Kolchin, B.A. Sevast'yanov, V.P. Chistyakov, Random Allocations, Wiley, New York, 1978.
[12] T. Larrabee, Y. Tsuji, Evidence for a satisfiability threshold for random 3CNF formulas, in: H. Hirsh et al. (Eds.), Proc. Spring Symp. on A.I. and NP-Hard Problems, Stanford CA, 1993, pp. 112–118.
[13] G. Logemann, M. Davis, D. Loveland, A Machine program for theorem proving, J. Assoc. Comput. Mach. 5 (1962) 267–270.
[14] P. Marquis, B. Mazure, Theory reasoning within implicant cover compilations, in: Proc. ECAI-96 Workshop on Advances in Propositional Deduction, 1996.
[15] E.L. McCluskey, Jr., Minimization of boolean function, Bell System Techniques 35 (1959) 1417–1444.
[16] D. Mitchell, B. Selman, H. Levesque, Hard and easy distribution of SAT problems, in: Proc. AAAI'92, July 1992, pp. 459–465.
[17] R. Motvani, P. Raghavan, Randomized Algorithms, Cambridge Univesity Press, New York, 1995.
[18] W.V.O. Quine, The problem of simplifying truth functions, Amer. Math. Mon. 59 (1952) 521–531.
[19] W.V.O. Quine, A Way to simplify truth functions, Amer. Math. Mon. 62 (1955) 627–631.
[20] W.V.O. Quine, On cores and prime implicants of truth functions, Amer. Math. Mon. 66 (1959) 755–760.
[21] J. Reiter, R. de Kleer, Foundation of assumption-based truth maintenance systems:preliminary report, in: Proc. 6th AAAI, 1987, pp. 183–188.
[22] R. Schrag, Compilation for critically constrained knowledge bases, in: Proc. 13th National Conf. on Artificial Intelligence (AAAI 96), 1996, to appear.
[23] N.M. Temme, Asymptotic estimates of stirling numbers, Studies in Applied Mathematics 89 (1993) 223–243.